Dr.WEB

Anti-virus for Windows servers

Administrator Manual

Жасағаны

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Защити созданное

Жасағаныңды қорға

Verteidige, was du erschaffen hast

Proteggi ciò che crei

Захисти створене

Defend what you create

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

Trademarks

Disclaimer

In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web Anti-virus for Windows servers
Version 11.0
Administrator Manual
9/6/2017

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya

Moscow, Russia

125040

Website: http://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

1. Introduction

Dr.Web Anti-virus for Windows servers provides multilevel protection of RAM, hard disks, and removable media against any kind of viruses, rootkits, Trojans, spyware, adware, hacktools, and all possible types of malicious objects from any external source.

The module architecture of Dr.Web is its significant feature. The anti-virus engine and virus databases are common for all components and different operating environments. At present, in addition to Dr.Web products for Windows, there are versions of anti-virus software for Novell® NetWare®, Macintosh®, Microsoft Windows Mobile®, Android®, Symbian®, BlackBerry®, and several Unix®-based systems (Linux®, FreeBSD®, Solaris®).

Dr.Web uses a convenient and efficient procedure for updating virus databases and program components via the Internet.

Dr.Web can detect and remove unwanted programs (adware, dialers, jokes, riskware, and hacktools) from your computer. To detect unwanted programs and perform actions with the files contained in the programs, anti-virus components of Dr.Web are used.

Each of Dr.Web anti-virus solutions for Microsoft® Windows® operating systems includes a set of the following components:

Dr.Web Scanner—an anti-virus scanner with a graphical interface that launches on demand or as scheduled and scans your computer for viruses and other malicious software.

Dr.Web Console Scanner—a command-line version of Dr.Web Scanner.

SpIDer Guard—an on-access anti-virus scanner that constantly resides in memory while scanning processes and files on start or creation and instantly detecting any malicious activity.

Updater—a component that allows registered users to receive updates of virus databases and other program files as well as automatically install them.

Dr.Web Agent—a utility that lets you set up and manage Dr.Web components.

Preventive Protection—a component that controls access to critical system objects and provides exploit prevention and integrity of running applications and files.

1.1 About This Manual

This User Manual describes installation and effective utilization of Dr.Web.

You can find detailed descriptions of all graphical user interface (GUI) elements in the Help system which can be accessed from any component.

This User Manual describes how to install the program and contains some words of advice on how to use it and solve typical problems caused by virus threats. Mostly, it describes the standard operating modes of the Dr.Web components (with default settings).

The Appendices contain detailed information on how to set up Dr.Web.

> ⚠ Due to constant development, program interface of your installation can mismatch the images given in this document. You can always find the actual documentation at http://download.drweb.com/doc.

1.2 Document Conventions

The following symbols and text conventions are used in this guide:

Convention	**Comment**
⚠	Warning about potential errors or any other important comment.
Signature	A new term or an accent on a term in its description.
<*key_file*>	Fields whose function names can be replaced with actual values.
Next	Names of buttons, windows, menu items, and other interface elements.
`C:\Windows\`	Names of files and catalogs, code examples.
Appendix A	Cross references to topics and hyperlinks to external resources.

1.3 Detection Methods

Doctor Web anti-virus solutions use several malicious software detection methods simultaneously, which allows them to perform thorough checks on suspicious files and control software behavior.

Detection Methods

Signature analysis

The scans begin with signature analysis that is performed by comparison of file code segments to the known virus signatures. A *signature* is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, Dr.Web anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. Dr.Web virus databases are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing

On completion of signature analysis, Dr.Web anti-virus solutions use the unique Origins Tracing method to detect new and modified viruses that use the known infection mechanisms. Thus, Dr.Web users are protected against such threats as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the Origins Tracing mechanism allows to considerably reduce the number of false triggering of the heuristic analyzer. Objects detected using the Origins Tracing algorithm are indicated with the `.Origin` extension added to their names.

Execution emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses, when the search against checksums cannot be applied directly, or is very difficult to be performed (due to the impossibility of building secure signatures). The method implies simulating the execution of an analyzed code by an emulator—a programming model of the processor and runtime environment. The emulator operates with protected memory area (emulation buffer), in which execution of the analyzed program is modelled instruction by instruction. However, none of these instructions is actually executed by the CPU. When the emulator receives a file infected with a polymorphic virus, the result of the emulation is a decrypted virus body, which is then easily determined by searching against signature checksums.

Heuristic analysis

The detection method used by the heuristic analyzer is based on certain knowledge (heuristics) about certain features (attributes) that might be typical for the virus code itself, and vice versa, that are extremely rare in viruses. Each attribute has a weight coefficient which determines the level of its severity and reliability. The weight coefficient can be positive if the corresponding attribute is indicative of a malicious code or negative if the attribute is uncharacteristic of a computer threat. Depending on the sum weight of a file, the heuristic analyzer calculates the probability of unknown virus infection. If the threshold is exceeded, the heuristic analyzer generates the conclusion that the analyzed object is probably infected with an unknown virus.

The heuristic analyzer also uses the FLY-CODE technology, which is a versatile algorithm for extracting files. The technology allows making heuristic assumptions about the presence of malicious objects in files compressed not only by packagers Dr.Web is aware of, but also by new, previously unexplored programs. While checking packed objects, Dr.Web anti-virus solutions also use structural entropy analysis. The technology detects threats by arranging pieces of code; thus, one database entry allows identification of a substantial portion of threats packed with the same polymorphous packager.

As any system of hypothesis testing under uncertainty, the heuristic analyzer may commit type I or type II errors (omit viruses or raise false alarms). Thus, objects detected by the heuristic analyzer are treated as “suspicious”.

While performing any of the abovementioned checks, Dr.Web anti-virus solutions use the most recent information about known malicious software. As soon as experts of Doctor Web anti-virus laboratory discover new threats, the update for virus signatures, behavior characteristics, and attributes is issued. In some cases, updates can be issued several times per hour. Therefore, even if a brand new virus passes through Dr.Web resident guards and penetrates the system, after an update it is detected on the list of processes and neutralized.

2. System Requirements

Before installing Dr.Web:

- Remove any anti-virus software from your computer to prevent possible incompatibility of resident Dr.Web components..
- In Windows Server 2016, disable Windows Defender manually, using group policies.
- Install all critical updates recommended by the operating system developer. If the operating system is no longer supported, then upgrade to a newer operating system.

Dr.Web can be installed and run on a computer that meets the following minimum requirements:

Component	Requirement
CPU	An i686-compatible processor.
Operating system	For 32-bit platforms: • Windows Server 2003 with Service Pack 1 • Windows Server 2008 with Service Pack 2 or higher For 64-bit platforms: • Windows Server 2008 with Service Pack 2 or higher • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016
Free RAM	Minimum 512 MB.
Hard disk space	750 MB for Dr.Web components. Files created during installation will require additional space.
Resolution	Minimum recommended screen resolution is 800x600.

Dr.Web Anti-virus for Windows Server is not compatible with Dr.Web for Microsoft Exchange Server, Dr.Web for IBM Lotus Domino, Dr.Web for Kerio WinRoute, Dr.Web for Kerio MailServer, Dr.Web for Microsoft ISA Server and Forefront TMG, Dr.Web for Qbik WinGate version 6.0 and earlier.

To ensure a correct operation of Dr.Web the following ports must be opened:

Purpose	Direction	Port numbers
To update (if the option to update using https is enabled)	outgoing	443
To update	outgoing	80
To send email notifications		25 or 465 (or depending on the settings of email notifications)
To connect to Dr.Web Cloud	outgoing	2075 (including UDP)

Other system requirements are similar to those for the corresponding operating system.

3. Installing, Removing, or Changing the Program

Before installing Dr.Web, note the system requirements and do the following:

- Install all critical updates released by Microsoft for the OS version used on your computer (they are available on the company update site at http://windowsupdate.microsoft.com).
- Check the file system with system utilities and remove the detected defects.
- Close all active applications.

> Remove any anti-virus software from your computer to prevent possible incompatibility of resident components.

3.1 Installation Procedure

> To install Dr.Web, the user must have administrative privileges.

There are two installation modes of Dr.Web anti-virus software:

- The usual mode;
- With command-line parameters.

Installation with command-line parameters

To install Dr.Web, enter in the command line the executable file name with necessary parameters (they affect installation in the background mode, installation language, reboot after installation).

Parameter	Description
lang	Language used for the installation. The value of this parameter is language in ISO 639-1 format.
reboot	Restart the computer automatically after installation is complete.
silent	Installation in the background mode.

For example, to start background installation of Dr.Web with reboot after the process completes, execute the following command:

```
drweb-11.0-srv-win.exe /silent yes /reboot yes
```

Usual installation

At any installation step, before the wizard starts copying files to your computer, you can do the following:

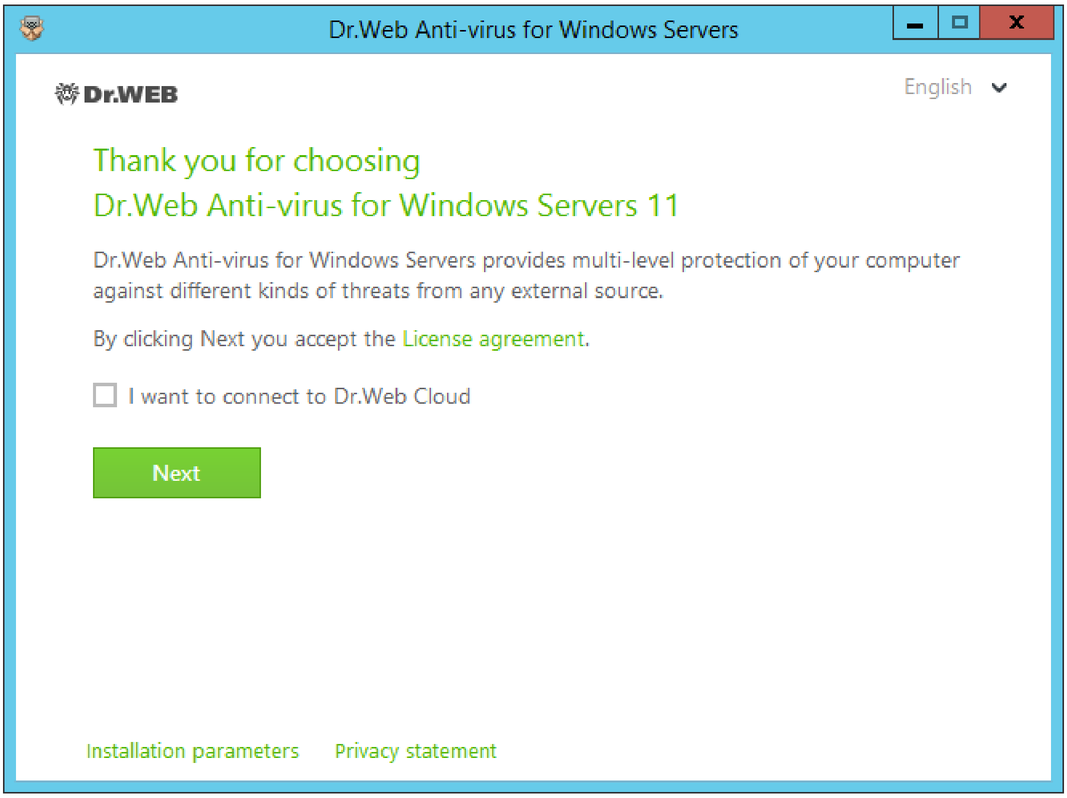
- Return to the previous step by clicking **Back**.
- Go to the next step by clicking **Next**.
- Abort installation by clicking **Undo**.

Installing Dr.Web

1. If other anti-virus software is installed on your computer, the Installation Wizard informs you on incompatibility between Dr.Web and another anti-virus product and offers to remove it.

   Before the installation starts, the Wizard checks if the installation file is the latest one. If a newer installation file exists, you will be offered to download it before the installation.

2. At this step, you are prompted to connect to Dr.Web cloud services that allow anti-virus components to use the newest information which is stored and updated on Doctor Web servers. This option is disabled by default.



Dr.Web Anti-virus for Windows Servers

Dr.WEB

English

Thank you for choosing
Dr.Web Anti-virus for Windows Servers 11

Dr.Web Anti-virus for Windows Servers provides multi-level protection of your computer against different kinds of threats from any external source.

By clicking Next you accept the License agreement.

□ I want to connect to Dr.Web Cloud

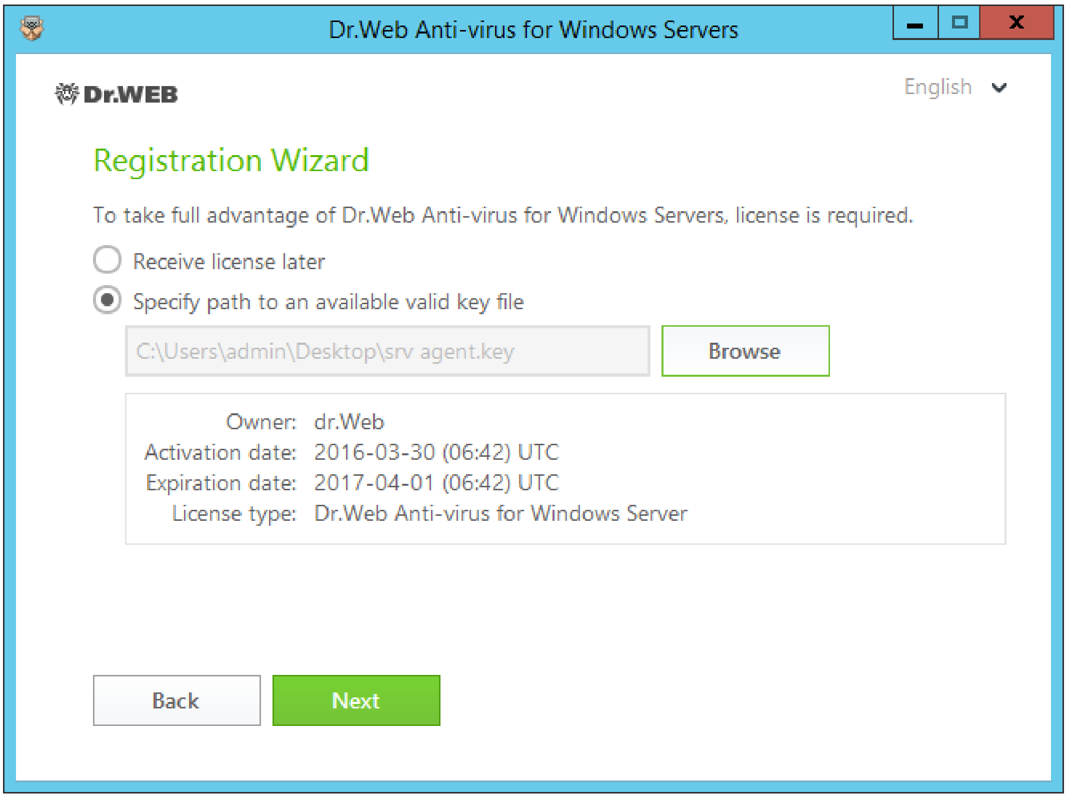
3. To select components you want to install, specify the installation path and configure other settings, click **Installation parameters**. The option is meant for experienced users. If you want to use default installation settings, go to step 4.
   - On the first tab, you can specify the components you want to install.
   - On the second tab, you can change the installation path.

- The last tab of the window has the enabled **Update during installation** option to download updates to virus databases and other program components. The tab prompts you to create shortcuts to Dr.Web.

To save the changes, click **OK**. To close the window without saving the changes, click **Undo**.

4. Click **Next**. Please note that by clicking the Next button you accept the terms of the License agreement.
5. The **Registration Wizard** informs you that a license is required for Dr.Web operation. Do one of the following:

- If a key file is present on the hard drive or removable media, click **Specify path to an available valid key file** and select the file in the open window. To change the path, click **Browse** and select another key file.
- To continue the installation without installing a key file, select **Receive license later**. If you select this option, none of the program components will operate until you get a valid key file.



Registration Wizard

To take full advantage of Dr.Web Anti-virus for Windows Servers, license is required.

○ Receive license later

● Specify path to an available valid key file

C:\Users\admin\Desktop\srv agent.key

Owner: dr.Web
Activation date: 2016-03-30 (06:42) UTC
Expiration date: 2017-04-01 (06:42) UTC
License type: Dr.Web Anti-virus for Windows Server

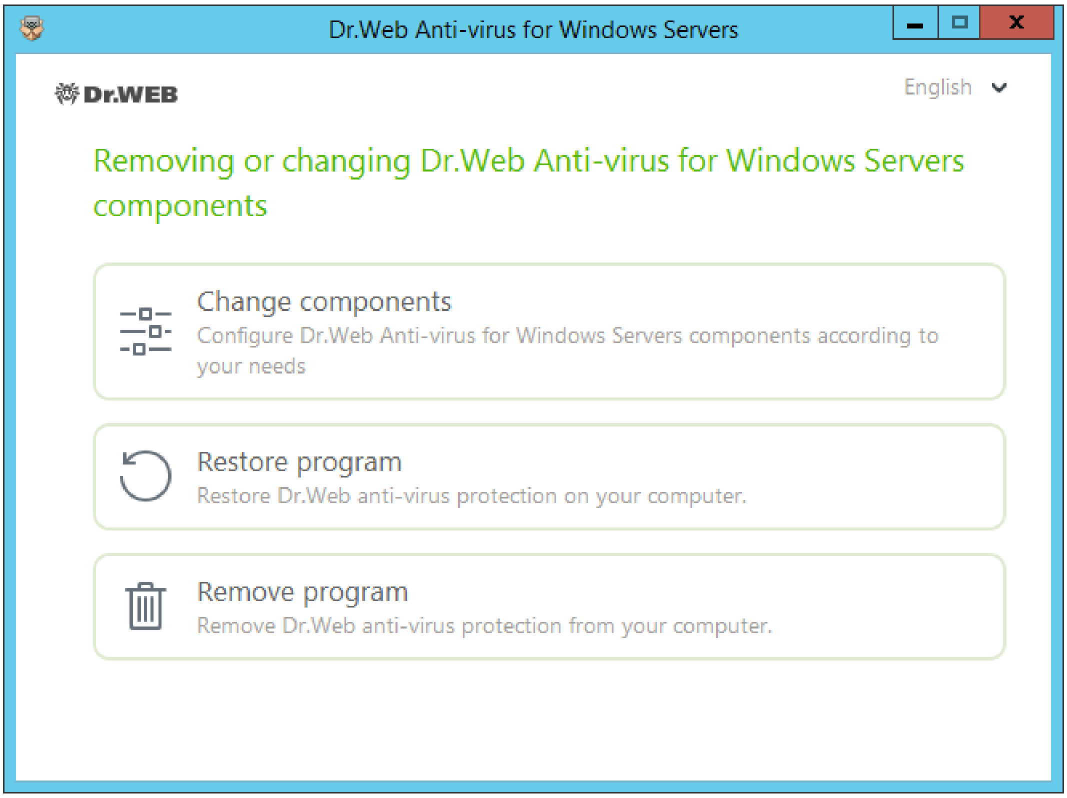
Click **Next**.

6. If you need to configure a proxy server, enable the option **Specify proxy server IP and port manually**. Click **Install**.
7. If you specified a key file and did not clear the **Update during installation** check box, the wizard updates virus databases and other Dr.Web components. Updating starts automatically and does not require any additional actions.
8. Restart your computer after the installation is complete.

3.2 Reinstalling or Removing the Program

After you uninstall Dr.Web, your computer will not be protected from viruses and other malware.

1. To uninstall Dr.Web or change its configuration by adding or removing individual components, run the standard Windows uninstall tool.
2. In the open window, select the program. To delete the program completely, click **Remove** and go to step 6. To change the configuration of Dr.Web by adding or removing certain components, click **Edit**. The window of the Installation Wizard opens.



Removing or changing Dr.Web Anti-virus for Windows Servers components

Change components
Configure Dr.Web Anti-virus for Windows Servers components according to your needs

Restore program
Restore Dr.Web anti-virus protection on your computer.

Remove program
Remove Dr.Web anti-virus protection from your computer.

3. To restore anti-virus protection on your computer, select **Restore program**.
4. To change the Dr.Web configuration, click **Change components**. In the open window, select check boxes of the components you want to add and clear check boxes of the components you want to remove. When you finish adjusting the component set, click **Apply**.

When removing components of Dr.Web, the **Disable Self-protection** window opens. Enter the displayed confirmation code and click **Install**.

5. To delete all installed components, select **Remove program**.

6. In the **Parameters to save** window, select check boxes of those components that you do not want to remove from your system. Saved objects and settings can be used by the program if it is installed again. By default, all options—**Quarantine**, **Dr.Web Settings Anti-virus for Windows Servers** and **Protected file copies**—are selected. Click **Install**.
7. In the next window, confirm deletion of Dr.Web by entering the displayed code and then click **Remove program**.
8. Once you reboot your computer, the changes are applied. You can snooze the reboot by clicking **Later**. Click **Restart now** to immediately complete the procedure of Dr.Web components deletion or modification.

4. Licensing

To use Dr.Web, activate a license. You can purchase a license with the product, on the official Doctor Web website or through authorized partners. A license allows to take advantage of all product features during the whole period. Parameters of the license are set in accordance with the software license agreement.

Key file

The use rights for Dr.Web are specified in the *key file*. Key files received within the product distribution kit are installed automatically.

The *key file* has the .key extension and contains the following information:

- List of licensed anti-virus components
- Licensed period for the product
- Availability of technical support for the user
- Other restrictions (for example, the number of remote computers allowed for simultaneous anti-virus check)

> By default, the key file is located in the Dr.Web installation folder. Dr.Web verifies the file regularly. Do not edit or modify the key file to avoid its corruption.
>
> If no valid key file is found, Dr.Web components are blocked.

A valid *key file* for Dr.Web satisfies the following criteria:

- License is not expired.
- Integrity of the key file is not violated.

If any of the conditions is violated, the *key file* becomes invalid and Dr.Web stops detecting and neutralizing malicious programs in files, memory, and email messages.

It is recommended to keep the *key file* until the license expires.

4.1 Activation Methods

You can activate your license in one of the following ways:

- Obtaining the key file during registration on the official website of Doctor Web.
- Specifying the path to the valid key file residing on your computer during installation or in the Registration Wizard window

Reactivating license

You may need to reactivate a license if the key file is lost.

> When reactivating a license, you receive the same key file as during the previous registration providing that the validity period is not expired.

When you reinstall the product or install it on several computers, if the license allows for that, you will be able to use the previously registered key file. Reactivation of the key file is not required.

The number of requests for a key file receipt is limited. One serial number can be registered not more than 25 times. If more requests are sent, the key file will not be delivered. In this case, to receive a lost key file, contact technical support describing your problem in detail, stating your personal data input during the registration and the serial number. The key file will be sent by technical support to your email address.

4.2 Renewing License

In some situations, for example, when the license expires or characteristics of the protected system change, you may need to renew or extend the Dr.Web license. If so, you should change the current key file. Dr.Web supports hot license update without stopping or reinstalling the product.

To change a key file

1. Open Registration Wizard. You can also purchase a new license or renew an existing one on your personal page on the Doctor Web official site. To visit the webpage, use the **My Dr.Web** option in the License Manager window or on the SpIDer Agent menu.
2. If the current key file is invalid, Dr.Web automatically switches to using the new key file.

4.3 Registration Wizard

SpIDer Agent checks whether you have a key file. If no key file is found, you are prompted to obtain a key file on the Internet.

You can specify a key file during the installation procedure. For that, select the **Specify the path to the valid key file** option at step 5 of the installation procedure.

You can also specify a key file after the product is installed on your system. For that, do the following:

1. Click the SpIDer Agent icon and select **License**. The License Manager window opens.
2. Click **Buy or activate new license**. The Registration Wizard window opens.

License activation

⚠ Users of Windows XP should indicate the valid key file (not the serial number) in order to activate Dr.Web license . If there is only serial number without the key file, it is necessary to activate it on the Doctor Web website.

If you have a key file for activation of a license, specify path to an available valid key file and click **Finish**.

New license

To purchase a new license, renew or extend your current license with a discount from Doctor Web online store, click **Buy**.

5. Getting Started

When Dr.Web is installed, the SpIDer Agent icon displays in the notification area.

> If SpIDer Agent is not running, select the **Dr.Web** application group on the Windows **Start** menu and then select **SpIDer Agent**.

The SpIDer Agent icon indicates the status of Dr.Web:

- —all necessary components are running and protect your computer.
- —Dr.Web self-protection or an important component is disabled, which compromises security of the anti-virus and your computer. Enable self-protection or the disabled component.
- —components are expected to start after the operating system startup process is complete, thus wait until the components start; or an error occurred while starting one of the main Dr.Web components, and your computer is at risk of virus infection. Check that you have a valid key file and, if required, install it.

Various notifications may appear over the SpIDer Agent icon if configured.

To open the menu, click the SpIDer Agent icon in the Windows notification area.

> To access the protection components and settings and to disable components, you need to have administrative privileges.

The SpIDer Agent menu allows to access the main management and setting functions of Dr.Web.

My Dr.Web. Opens your personal webpage on the Doctor Web official website. This page provides you with information on your license including usage period and serial number, allows to renew the license, contact technical support, and so on.

License. Opens License Manager.

Tools. Opens a submenu providing access to:

- Data Loss Prevention
- Anti-virus Network
- Quarantine Manager
- Go to Support.

Protection Components. Quick access to the protection components list where you can enable or disable each of the components.

Update. Information about actuality of the components or virus databases. Launches the update.

Scanner. Quick access to launching different kinds of scanning.

Operation mode . Allows to switch between user mode and administrator mode. By default, Dr.Web starts in restricted user mode, which does not provide access to Settings and settings of Protection components. To switch to another mode, click the lock. If UAC is enabled, operating system will prompt a request for administrative privileges. Besides, you also need to enter the password to change the mode, if you set **Protect Dr.Web settings with a password** option on the Settings window.

Statistics . Opens statistics on the components operations in the current session including the number of scanned, infected and suspicious objects, actions performed, and so on.

Settings . Opens a window with access to the main settings, protection components settings, and exclusions.

To access the component settings and open your personal webpage **My Dr.Web**, you also need to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the Settings window.

If you forgot your password for the product settings, contact technical support.

Help . Opens the help file.

5.1 Testing the Anti-virus

The EICAR (European Institute for Computer Anti-Virus Research) test file helps to test performance of anti-virus programs that detect viruses using signature analysis.

For this purpose, most of the anti-virus software vendors generally use a standard test.com program. This program was designed specially so that users could test reaction of newly-installed anti-virus tools to virus detection without compromising security of their computers. Although the test.com program is not actually a virus, it is treated by the majority of anti-viruses as if it were a virus. On detection of this file, Dr.Web reports the following: `EICAR Test File (Not a Virus!)`. Other anti-virus tools alert users in a similar way.

The test.com program is a 68-byte COM-file that prints the following line on the console when executed: `EICAR-STANDARD-ANTIVIRUS-TEST-FILE!`

The file test.com contains the following character string only:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

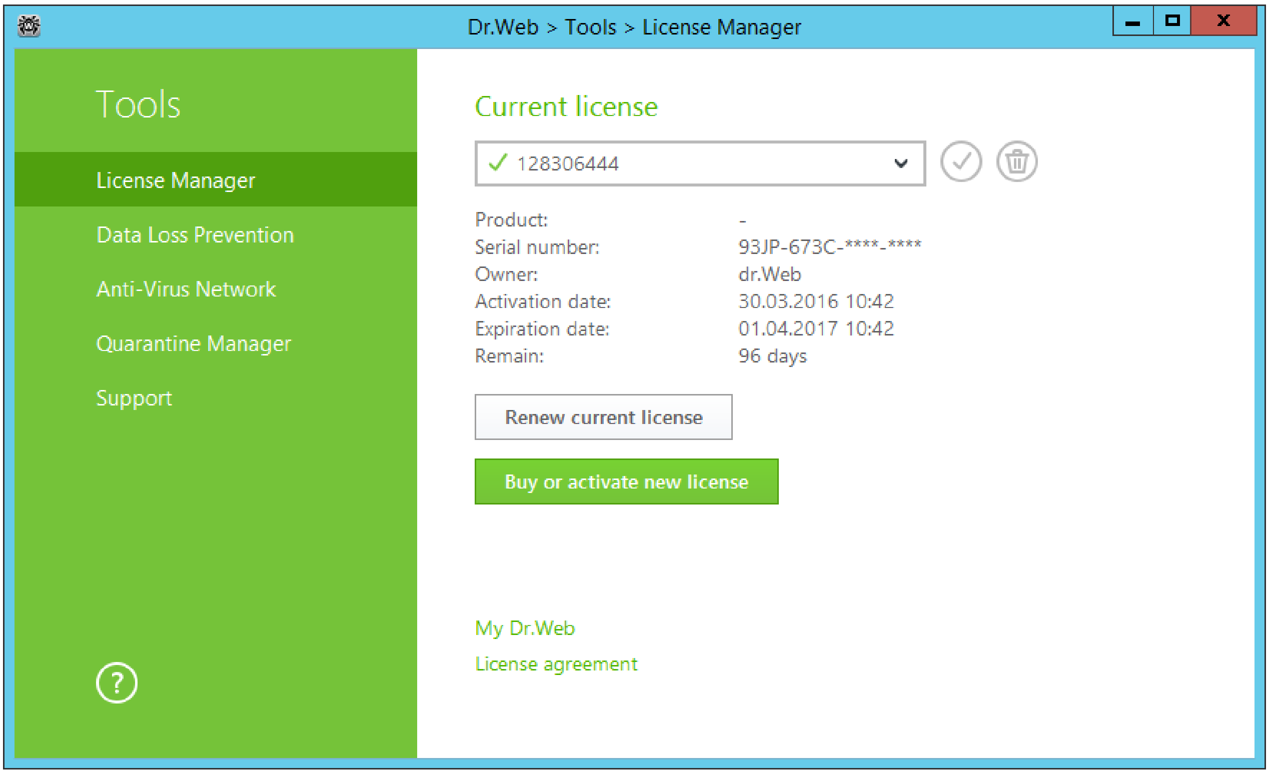
To make your own test file with the “virus”, create a new file with this line and save it as test.com.

When running in the Optimal mode, SpIDer Guard does not terminate execution of an EICAR test file and the file is not processed as malicious since it does not pose any actual threat to your system. However, if you copy or create such a file in your system, it will be detected by SpIDer Guard and moved to Quarantine by default.

6. Tools

6.1 License Manager

In this window, you can view all Dr.Web licenses for your computer. You can also modify the current license, renew it or purchase a new license and activate it.



Dr.Web > Tools > License Manager

Current license

✓ 128306444

Product:	-
Serial number:	93JP-673C-****-****
Owner:	dr.Web
Activation date:	30.03.2016 10:42
Expiration date:	01.04.2017 10:42
Remain:	96 days

To view information on a license that is not currently in use, select it from the drop-down list. In the administrator mode, click 🗑 to delete the selected license or click ✓ to set it as current. Please note that the current license cannot be deleted.

Once you click **Buy or activate new license**, the Registration Wizard window opens providing you with necessary instructions on how to proceed.

Once you click **Renew current license**, the program will open the page on the Doctor Web website where all parameters of the current license will be transmitted.

Advanced

Opens your personal webpage on the Doctor Web official website. This page provides you with information on your license including usage period and serial number, allows to renew the license, contact technical support, and so on.

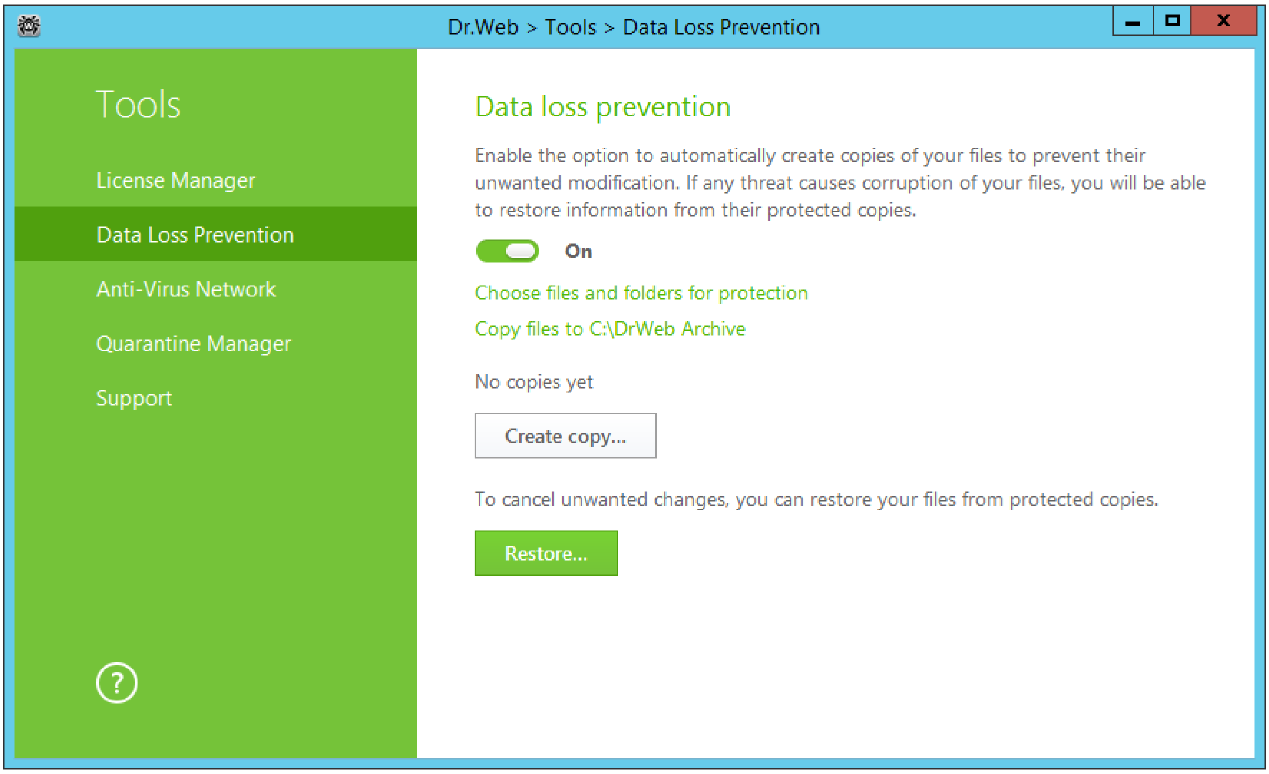
The **License agreement** link opens the license agreement on the Doctor Web official website.

6.2 Data Loss Prevention

You cannot change data loss prevention parameters or restore files from copies in user mode. For this actions, switch to administrator mode.

To protect important files from being changed by malicious software, enable the **Data Loss Prevention**. With this function, you can make copies of files that reside in the specified folders.

If a file is blocked, it will not be copied.



Data loss prevention

Enable the option to automatically create copies of your files to prevent their unwanted modification. If any threat causes corruption of your files, you will be able to restore information from their protected copies.

On

Choose files and folders for protection

Copy files to C:\DrWeb Archive

No copies yet

Create copy...

To cancel unwanted changes, you can restore your files from protected copies.

Restore...

To configure list of files and folders for protection

Click the **Choose files and folders for protection** link to specify the objects for which protected copies will be created:

- to add a file or a folder, click ⊕ and select the required object;
- to remove an object from the list, select the corresponding item from the list and click 🗑.

You may change the objects list at any time.

Parameters for creating a copy

Click the link **Copy files to C:\DrWeb Archive**. Specify the required parameters in the appeared window.

1. Set common parameters for copies:
   - Specify a disk for storage of copies.
   - Specify frequency of copy creation. After the chosen interval, Dr.Web will inspect the specified objects for changes and create a copy if any changes have been made.
   - If necessary, block the copy creation option when running on battery power.
2. Specify a limit of available disk space:
   - Set maximum disk space used for storage of copies.
   - If necessary, specify a limit on number of copies.
   - Select one of the actions: if any of the specified limits is exceeded, copies are not created, or they overwrite the existing ones (starting from the oldest copy).

Removal of created copies

You may also delete copies to free up some disk space (deleting the copies will not affect the original files). To do that click **Copy files to C:\DrWeb Archive**, then click **Delete copies**.

Restoring files

If your files were corrupted, you can restore their copies created by a certain date. To do that, click the **Restore** button in the main window and then click **Next**. In the window displayed, select the required date and all copies that were available for the date will be restored to the specified folder.

Start creating copies manually

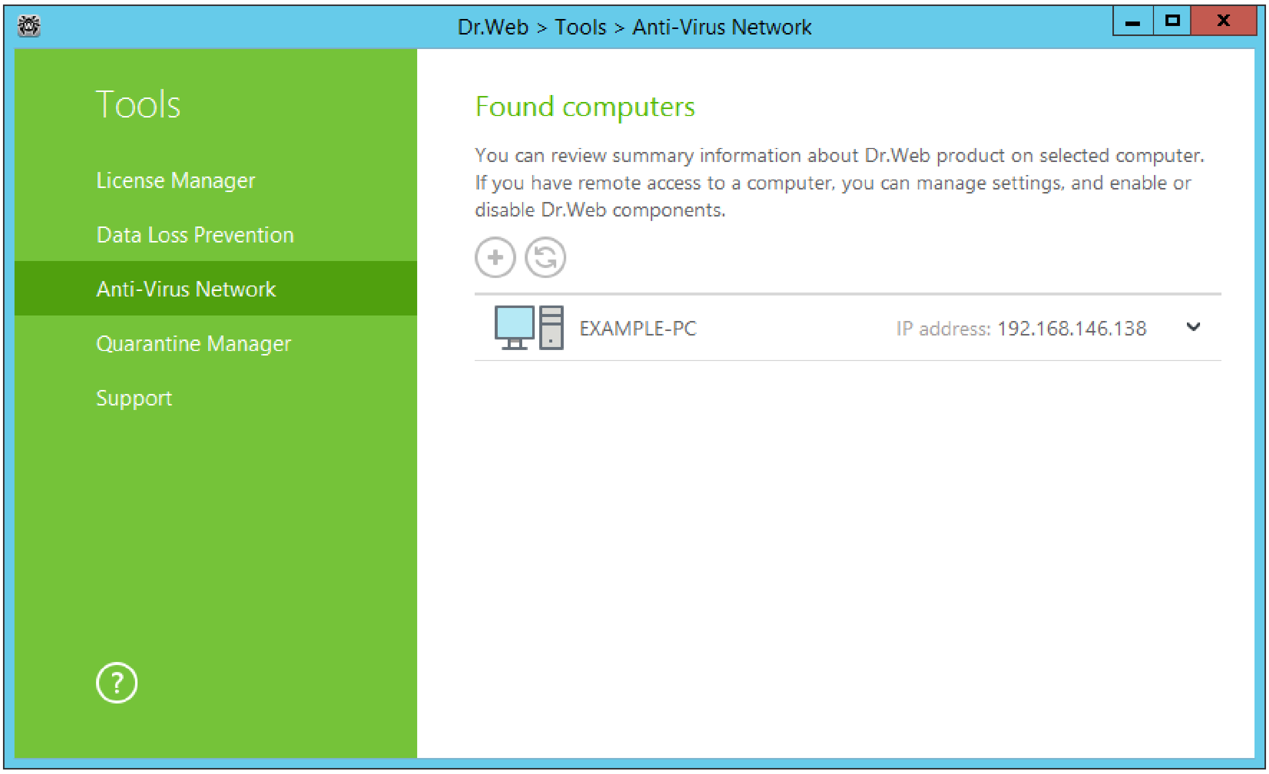
To start creation of protected copies manually, click the **Create copy** button in the main window. In the window displayed, specify the description for the new copy.

> ⚠ To ensure correct operation the **Data Loss Prevention** system, you need to have at least 20 GB free on the disk that is selected for storing protected copies.

6.3 Anti-virus Network

This section allows to manage Dr.Web Anti-virus for Windows, Dr.Web Anti-virus for servers, or Dr.Web Security Space within one product version on other computers of your network.

To access Dr.Web remote control, click the SpIDer Agent icon in the notification area, select **Tools**, and then select **Anti-Virus Network**.



Dr.Web > Tools > Anti-Virus Network

Found computers

You can review summary information about Dr.Web product on selected computer. If you have remote access to a computer, you can manage settings, and enable or disable Dr.Web components.

EXAMPLE-PC IP address: 192.168.146.138

To access a remote anti-virus, select the computer from the list and click **Connect...**. Enter the password specified in the settings of the remote anti-virus. An icon for remote SpIDer Agent appears in the notification area, and the notification about established connection will be displayed.

You can view settings, enable or disable components, and configure their settings. Anti-Virus Network, Quarantine and Scanner are not available. Dr.Web Firewall settings and statistics are not available as well, but you can enable or disable this component (if you accessed Dr.Web Anti-virus for Windows or Dr.Web Security Space). Also you can select the **Disconnect** item to terminate the remote connection.

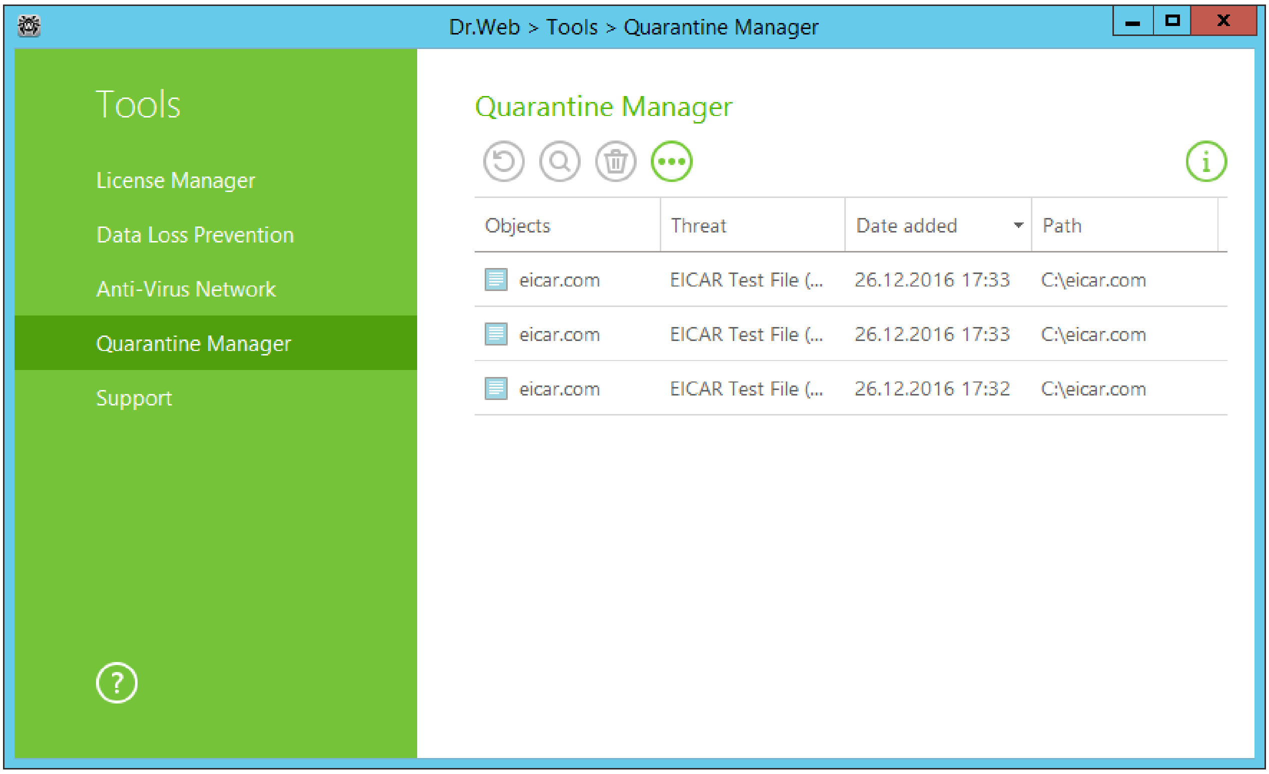
If the required computer is not on the list, you can try to add it manually. For this, click ⊕ and enter an IP-address.

> ⚠ You can establish only one connection with a remote Dr.Web product. If one connection is already established, the **Connect...** button is disabled.

Computers are listed if Dr.Web products installed on these computers allow remote connection. You can allow connection to your Dr.Web on the Anti-Virus Network page in Main settings.

6.4 Quarantine Manager

Quarantine Manager contains information on the Quarantine component of Dr.Web which serves for isolation of files that are suspected to be malicious. The Quarantine also stores backup copies of files processed by Dr.Web.



Objects	Threat	Date added	Path
eicar.com	EICAR Test File (...	26.12.2016 17:33	C:\eicar.com
eicar.com	EICAR Test File (...	26.12.2016 17:33	C:\eicar.com
eicar.com	EICAR Test File (...	26.12.2016 17:32	C:\eicar.com

Use Quarantine Manager settings to select the isolation mode for infected objects detected on portable data carriers. When this option is enabled, detected threats are moved to the folder on this data carrier without being encrypted. The Quarantine folder is created only when the data carrier is accessible for writing. The use of separate folders and omission of encryption on portable data carriers prevents possible data loss.

To open this window, click the SpIDer Agent icon in the notification area, select **Tools**, and then select **Quarantine Manager**.

The central table lists the following information on quarantined objects:

- **Objects**—name of the quarantined object.
- **Threat**—malware class of the object, which is assigned by Dr.Web when the object is quarantined.
- **Date added**—date and time when the object was moved to the Quarantine.
- **Path**—full path to the object before it was quarantined.

Quarantine Manager displays objects that can be accessed by your user account. To view hidden objects, you need to have administrator privileges.

In the objects context menu, the following buttons are available:

- **Restore**—move the file to the selected folder and specify a new file name.

> ⚠ Use this option only when you are sure that the selected object is not harmful.

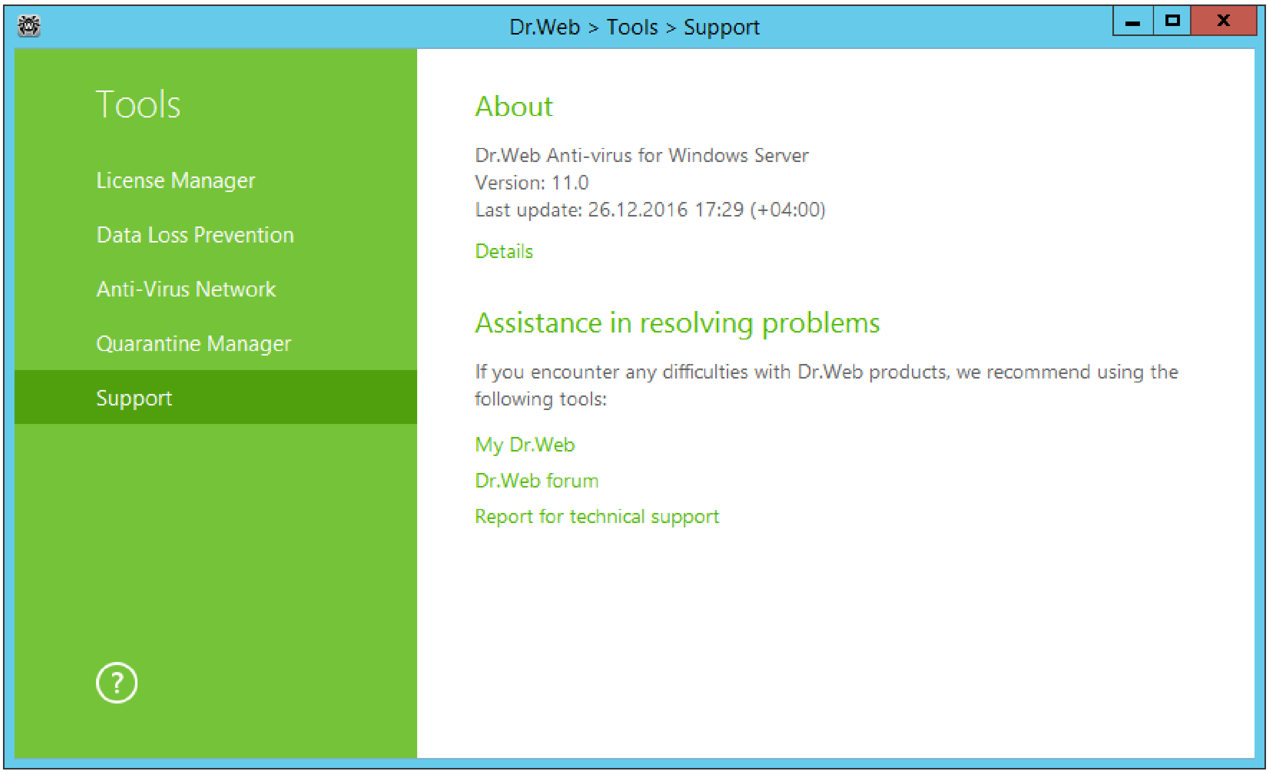
- **Scan**—scan the file in quarantine again.
- **Remove**—delete the file from the Quarantine and from the system.

You can also access these settings by right-clicking the selected object or several selected objects.

To delete all objects from the Quarantine, click ⋯ and select **Delete all** from the drop-down list.

6.5 Support

This section provides information on the product version, components, the last update date,, and the useful links that may help you to resolve issues or solve problems encountered while using Dr.Web.



About

Dr.Web Anti-virus for Windows Server
Version: 11.0
Last update: 26.12.2016 17:29 (+04:00)

Details

Assistance in resolving problems

If you encounter any difficulties with Dr.Web products, we recommend using the following tools:

My Dr.Web
Dr.Web forum
Report for technical support

In case of questions, we recommend using one of the following tools:

My Dr.Web. Opens your personal webpage on the Doctor Web official website. This page provides you with information on your license including usage period and serial number, allows to renew the license, contact technical support, and so on.

Dr.Web forum. Opens Dr.Web forum at http://forum.drweb.com.

Report for technical support. Launches the wizard that will help you to create a report containing important information on your system configuration and computer working.

If you have not found a solution for the problem, you can request direct assistance from Doctor Web technical support by filling in the web from at http://support.drweb.com/.

For regional office information, visit the Doctor Web official website at http://company.drweb.com/contacts/moscow.

6.5.1 Report Wizard

When contacting Doctor Web technical support, you can generate a report on your operating system and Dr.Web operation.

The report will be stored as an archive in the Doctor Web subfolder of the %USERPROFILE% folder.

To generate a report, click the corresponding button. The report will include the following information:

1. Technical information about the operating system:
   - General information about your computer
   - Running processes
   - Scheduled tasks
   - Services, drivers
   - Default browser
   - Installed applications
   - Policies
   - HOSTS file
   - DNS servers
   - System event log
   - System directories
   - Registry branches
   - Winsock providers
   - Network connections
   - Dr.Watson logs
   - Performance index
2. Information about Dr.Web anti-virus solutions.

3. Information about the following plug-ins:
   - Dr.Web for IBM Lotus Domino
   - Dr.Web for Kerio MailServer
   - Dr.Web for Kerio WinRoute

Information about Dr.Web anti-virus solutions is located in Event Viewer, in **Application and Services Logs** → **Doctor Web**.

Report generation from command line

To generate a report, use the following command:

```
/auto
```

For example: `Exampledwsysinfo.exe /auto`

The report will be stored as an archive in the Doctor Web subfolder of the %USERPROFILE% folder.

You can also use the command:

`/auto/report`: [<*full path to the archive*>]

where

- <*full path to the archive*>—path to the report file.

For example: `Exampledwsysinfo.exe /auto /report:C:\report.zip`

7. Update

The anti-virus solutions of Doctor Web use Dr.Web virus databases to detect malicious software. These databases contain details and signatures for all virus threats known at the moment of the product release. With the updates, Dr.Web receives information required to detect and block new viruses and sometimes to cure the infected files that were considered unrecoverable before.

From time to time, updates include enhancements to anti-virus algorithms in the form of executable files and libraries. The experience of Dr.Web anti-virus protection helps to fix any bugs in software and to update help system and documentation.

To ensure the virus databases and software algorithms being most up to date, Doctor Web provides you with regular updates to virus databases and product components, which are distributed via the Internet. Dr.Web Update helps you download and install updates of virus databases and program modules during the licensed period.

Update start

During update, Dr.Web downloads and installs all updated files that correspond to your version of Dr.Web and upgrades Dr.Web when a newer version is released.

⚠ For Dr.Web to update, you need a connection to the Internet, to the update mirror (local or network folder), or to the Anti-virus network with at least one computer that has an update mirror set.

All necessary parameters can be defined on the **Update** page of Dr.Web Main settings.

Start from the SpIDer Agent menu

Click the SpIDer Agent icon and select **Update**. This opens information on relevance of Dr.Web virus databases and other components as well as the date of their last update. Start updating by clicking **Refresh**.

Start from the command line

Open the Dr.Web installation folder (%PROGRAMFILES%\Common Files\Doctor Web\Updater) and run the drwupsrv.exe file. The list of command-line parameters can be found in Appendix A.

Automatic start

If launched automatically, Dr.Web installs updates silently and logs all changes into the dwupdater.log file located in the %allusersprofile%\Doctor Web\Logs\ folder.

> ⚠ After an update of executable files, drivers, or libraries, a program restart may be required. In such cases, an appropriate warning displays.

8. Dr.Web Scanner

Dr.Web Scanner for Windows allows you to run anti-virus scans of disk boot sectors, random access memory (RAM), and both separate files and objects enclosed within complex structures (archives, containers, or email attachments). The program uses all detection methods to detect viruses and other malicious software. By default, Dr.Web Scanner checks all files for viruses using both the virus database and the heuristic analyzer (a method based on the general algorithms of virus developing allowing to detect the viruses unknown to the program with a high probability). Executable files compressed with special packers are unpacked when scanned. Files in archives of all commonly used types (ACE, ALZIP, AR, ARJ, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, etc.), in containers (1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM, etc.), and in mailboxes of mail programs (the format of mail messages should conform to RFC822) are also checked.

On detection of a malicious object, Dr.Web Scanner only informs you about it. Information on all infected or suspicious objects displays in the table where you can manually select a necessary action. You can apply default actions to all detected threats or select the required reaction to a certain object.

The default settings are optimal for most cases. However, if necessary, you can modify the suggested actions in the Dr.Web Scanner settings window. Please note that you can specify a custom action for each detected threat after the scan is complete, but common reaction for a particular threat type should be configured beforehand.

8.1 Scanning Your System

To select the scan mode

> ⚠ When using Windows Server 2003 or later operating systems, it is recommended to run Dr.Web Scanner with administrative privileges. Otherwise, all folders and files (including system folders) that are not accessible to an unprivileged user will not be scanned.

1. Click the SpIDer Agent menu and select **Scanner**. The menu of quick access to different scan modes opens.
2. Click the **Custom** item to scan only selected objects. The Dr.Web Scanner window opens.
3. Click the **Express** or **Full** item to run the corresponding scan mode.

To launch Scanner with default settings to scan a certain file or folder, select **Check with Dr.Web**.

Configuring Dr.Web Scanner

To configure Dr.Web Scanner and its reactions to detected threats, go to **Settings** → **Protection Components** → **Scanner**.

Scan modes

Express scan

In this mode, Scanner checks the following:

- Boot sectors of all disks
- Random access memory
- Boot disk root folder
- Windows system folder
- User documents folder (“My Documents”)
- Temporary files
- System restore points
- Presence of rootkits (if the process is run with administrative privileges)

> ⚠ Scanner does not check archives and email files in this mode.

Full scan

In this mode, random access memory and all hard drives (including boot sectors of all disks) are scanned. Moreover, Scanner runs a check for rootkits.

Custom scan

In this mode, you can select objects to be scanned, for example, any files and folders and such objects as random access memory, boot sectors, and so on. To start scanning selected objects, click **Start scanning**. To select objects, click ⊕.

Scan process

When scanning starts, the **Pause** and **Stop** buttons become available. During scanning, you can do the following:

- To pause scanning, click **Pause**. To resume scanning after pause, click **Resume**.
- To stop scanning, click **Stop**.

> ⚠ The **Pause** button is not available while processes and RAM are scanned.

8.2 Actions upon Detection

If any viruses or computer threats of other types are detected during scanning, Dr.Web Scanner informs you about them and recommends the most effective actions to neutralize them. You can neutralize all detected threats at once by clicking **Neutralize**. In this case, Dr.Web Scanner applies the most effective actions according to its configuration and threat type.

By clicking **Neutralize**, you apply actions to in the table. neutralize all objects by default once scanning completes. If necessary, you can select objects or groups of objects manually. To select a group of objects, you can use CTRL and SHIFT keys. To select actions for neutralizing threats, right-click one or several selected objects and choose an option from the context menu.

To select an action

1. Where necessary, select a custom action from the drop-down list in the **Action** field. By default, Dr.Web Scanner selects a recommended action.
2. Click **Neutralize**. Dr.Web Scanner applies actions to the selected threats.

There are the following limitations:

- For suspicious objects, curing is impossible.
- For objects which are not files (boot sectors) moving and deletion is impossible.
- For files inside archives, installation packages or attachments, no actions are possible.

The detailed report on program operation is stored in the dwscanner.log file that is located in % USERPROFILE%\Doctor Web folder.

Column name	Description
Object	This table column contains the name of an infected or suspicious object (either a file name if a file is infected, or **Boot sector** if a boot sector is infected, or **Master Boot Record** if an MBR of the hard drive is infected).
Threat	The names of viruses or virus modifications as per the internal classification of Doctor Web (modification of a known virus is a code resulting from such alteration of a known virus which can still be detected but cannot be cured with the algorithms applied to the initial virus). For suspicious objects, the following is displayed: indication that the object “is possibly infected” and the type of a possible virus according to the classification used by the heuristic analyzer.
Action	Click an arrow on this button to select a custom action for a detected threat (by default, Dr.Web Scanner offers the most effective action). You can apply the displayed action separately to each threat by clicking this button.
Path	The full paths to the corresponding files.

If you enabled the **Neutralize detected threats** option on the settings page of Dr.Web Scanner to configure **After scanning**, threats will be neutralized automatically.

8.3 Command-Line Scanning Mode

You can run Dr.Web Scanner in the command-line mode that allows to specify settings of the current scanning session and the list of objects for scanning as additional parameters. Automatic activation of the Scanner according to schedule is performed in this mode.

To run scanning from command line

For that purpose, use the following command:

[<*path_to_program*>]`dwscanner` [<*switches*>] [<*objects*>]

where

- <*objects*> is a placeholder for the list of objects to be scanned.
- <*switches*> are command-line parameters that specify settings of Scanner. If no switches are defined, scanning is performed with the settings specified earlier (or with the default settings if you have not changed them).

The list of objects for scanning can be empty or contain several elements separated by spaces. The most common scan modes are as follows:

- `/FAST`—perform an express scan of the system.
- `/FULL`–perform a full scan of all hard drives and removable media (including boot sectors).
- `/LITE`—perform a basic scan of random access memory and boot sectors of all disks as well as run a check for rootkits.

Switches are command-line parameters that specify program settings. If no switches are defined, scanning is performed with the settings specified earlier (or with the default settings if you have not changed them). Switches begin with the forward slash (/) character and are separated by blanks as other command-line parameters.

8.4 Console Scanner

Dr.Web includes Console Scanner which allows you to run scanning from the command line and provides advanced settings.

Console Scanner moves suspicious files to Quarantine.

To run Console Scanner

The command syntax to launch Console Scanner is as follows:

[<*path_to_program*>]`dwscancl` [<*switches*>] [<*objects*>],

where

- <*objects*> is a placeholder for the list of objects to be scanned.
- <*switches*> is a placeholder for command-line parameters that configure Console Scanner operation.

Parameter begins with the forward slash (/) character; several parameters are separated by spaces. The list of objects for scanning can be empty or contain several elements separated by spaces.

All Console Scanner switches are listed in Appendix A.

After the operation is complete, Console Scanner returns one of the following codes:

0—scanning completed successfully; infected objects were not found;

1—scanning completed successfully; infected objects were detected;

10—invalid keys are specified;

11—key file is not found or does not support Console Scanner;

12—Scanning Engine did not start;

255—scanning was aborted by user request.

8.5 Automatic Launch of Scanning

During installationof Dr.Web, an anti-virus scan task is automatically created in the Task Scheduler (the task is disabled by default).

To view task settings, open **Control Panel** (extended view) → **Administrative Tools** → **Task Scheduler**.

From the task list, select the scan task. You can enable the task, adjust trigger time, and set required parameters.

On the **General** page, you can review general information and security options on a certain task. On the **Triggers** and **Conditions** pages, various conditions for task launching are specified. To review event log, open the **Log** page.

You can also create your own anti-virus scan tasks. For details on the system scheduler operation, please refer to the Help system and Windows documentation.

9. Settings

To access the main settings, open the SpIDer Agent in administrator mode and click **Settings** .

Password protection

To restrict access to Dr.Web settings on your computer, enable the **Protect Dr.Web settings with a password** option. In the open window, specify the password that will be required for configuring Dr.Web, confirm it, and click **OK**.

> If you forgot your password for the product settings, contact technical support.

Manage settings

To restore default settings, select **Reset settings** from the drop-down list.

If you want to use settings of the anti-virus that you already configured on another computer, select **Import** from the drop-down list.

If you want to use your settings on other computers, select **Export** from the drop-down list. Then apply them on the same page of another anti-virus.

10. Main Settings

To access the main Dr.Web settings, open the SpIDer Agent menu in administrator mode, run **Settings** and go to **Main**.

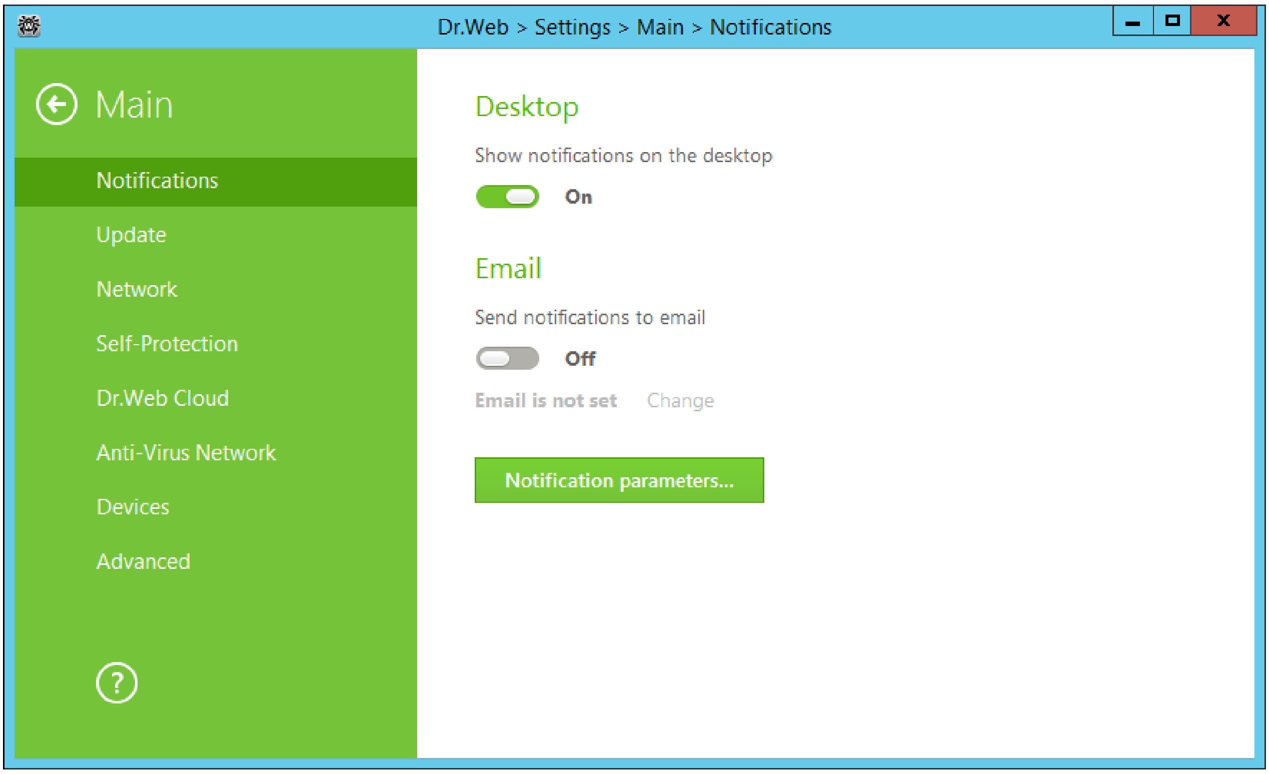
> To access the main Dr.Web settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the Settings window.

Centralized settings adjustment allows you to configure main settings of the anti-virus package.

10.1 Notifications

Pop-up notifications

Enable the appropriate option to get pop-up notifications above the SpIDer Agent icon in the Windows notification area.



Desktop

Show notifications on the desktop

On

Email

Send notifications to email

Off

Email is not set Change

Email notifications

To receive email notifications about events, do the following:

1. Enable the **Send notifications to email** option.

2. Specify the email address that you want to use for receiving notifications in the appeared window. You will need to confirm this email address at step 7.
3. Click **Next**.
4. Specify the data of the account that will be used to send notifications.
   - Select the mail server from the list and enter your account login and password.
   - If the required mail server is not on the list, select **Set manually**. In the open window, fill in the fields.

Option	Description
SMTP server	Specify the outgoing (SMTP) server for Dr.Web to use when sending email notifications.
Port	Enter the port for Dr.Web to use when connecting to the mail server.
Login	Enter the login for Dr.Web to use when connecting to the mail server.
Password	Enter the password for the login to be used when connecting to the mail server.
Use SSL/TLS	Select this check box to use SSL/TLS encryption when sending messages.
NTLM authentication	Select this check box to use NTLM authentication when connecting to the mail server.

5. Click **Send a test message** if you want to make sure that all the details are specified correctly. The message is forwarded to the email address that will be used to send notifications (specified at step 4).
6. Click **Next**.
7. Enter the conformation code that was sent to the email address specified at step 2. If you do not receive the message within 10 minutes, click **Send the code again**. If you do not enter the code, notifications to this email address will not be sent.
8. To change the email address and other parameters, click **Edit** and repeat all the actions starting from step 2.
9. Click **Notifications parameters** and set the required notification types. By default, all types of email notifications are disabled.

Notification parameters

1. Click **Notifications parameters**.
2. Select types of notifications that you want to receive and select the corresponding check boxes. To display pop-up notifications, select check boxes in the **Desktop** column. To receive mail notifications, select check boxes in the **Mail** column.

Notification type	Description
Threat notifications	Select to be notified on threats detected by SpIDer Guard. Clear if you do not want to be notified. By default, these notifications are enabled.
Critical notifications	Select to be notified on the following critical issues: • Failures to make a protected copy. Clear if you do not want to be notified on the issues listed above. By default, these notifications are enabled.
Major notifications	Select to be notified on the following major issues: • Device is blocked. • An attempt to access a protected object is blocked by Preventive Protection. • Attempt to change system date and time is blocked. • New version is available. • Virus databases are out of date. Clear if you do not want to be notified on the issues listed above. By default, these notifications are enabled.
Minor notifications	Select to be notified on the following minor issues: • Successful update. • Update failures.. Clear if you do not want to be notified on the issues listed above. By default, these notifications are disabled.
License	Select to be notified on the following issues: • Your license period is expiring. • Valid license is not found. • The current license is blocked.

3. If necessary, configure additional parameters:

Option	Description
Do not show notifications in full-screen mode	Select this check box to hide notifications when an application is running in full-screen mode on your computer (e.g., a game or a movie). Clear this check box to display notifications regardless of the mode.

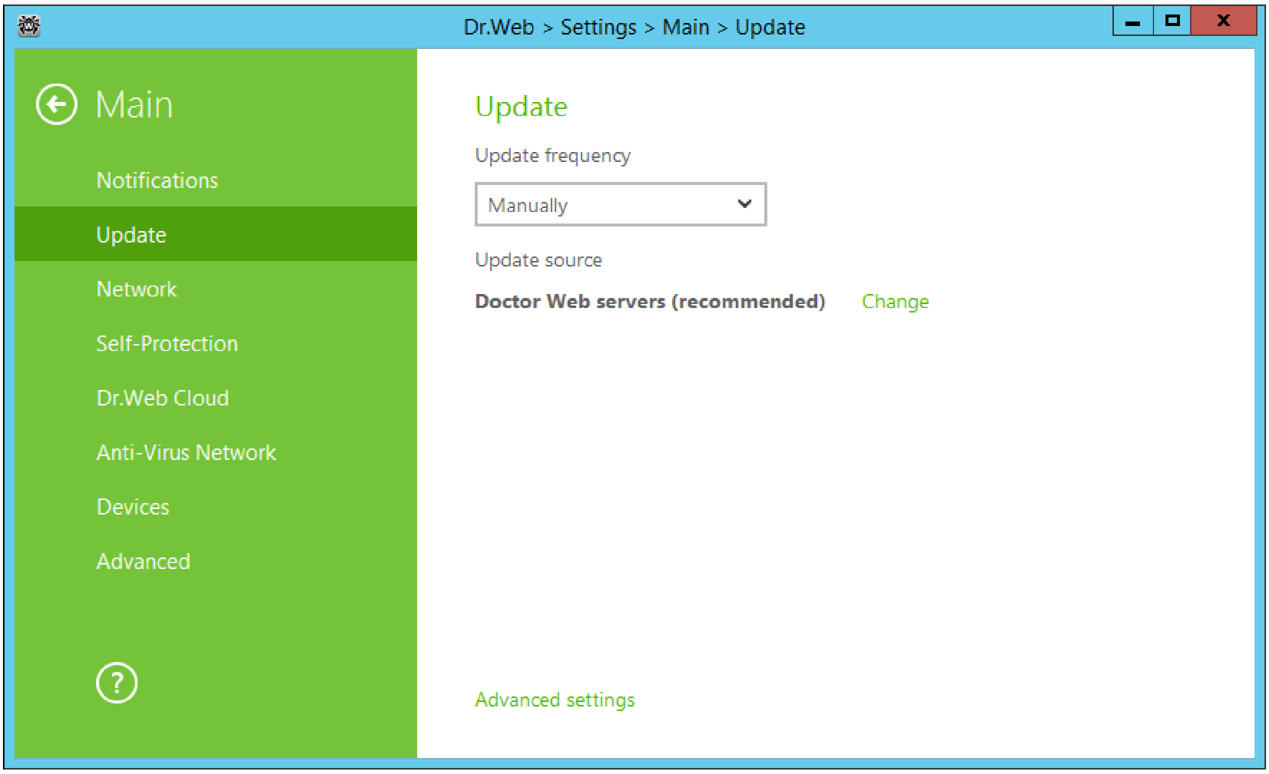
4. If you selected one or more email notifications, configure sending emails from your computer.

Notifications on the following issues are not included in any of the specified groups and are always displayed to the user:

- Priority updates installed and restart is required.
- To finish neutralizing threats, restart the computer.
- To enable or disable the hypervisor, restart the computer.
- Request for allowing a process to modify an object.
- Successful connection to a remote computer in the Anti-virus Network.

10.2 Update

On this page, you can configure various Dr.Web update parameters, such as components that should be updated, an updating source, update period, proxy server, and update mirror.



Dr.Web > Settings > Main > Update

Update

Update frequency

Manually

Update source

Doctor Web servers (recommended) Change

Advanced settings

General update settings

Update frequency. Specify the frequency to check for updates. The default value (30 minutes) is optimal to keep information on threats up to date.

Update source. To select an update source, click **Change Edit**. In the open window, select one of the following update sources:

- **Doctor Web servers (recommended)**. This source is selected by default.

- **Local or network folder**—update from local or network folder where updates have been copied. To specify the path to the folder, click **Browse** and select the required folder, or enter the address manually. Enter the user name and password if necessary.
- **Anti-Virus Network**—updates are to be downloaded from a local network computer if Dr.Web product is installed and update mirror is created on it.

If you want to download updates via a secure protocol, select the **Use HTTPS connection** check box.

To configure additional settings

Updating components. You can choose one of the following ways of downloading the update:

- **All (recommended)**, when updates are downloaded both for Dr.Web virus databases and anti-virus engine and for other program components of the Dr.Web.
- **Only virus databases**, when only the updates for Dr.Web virus databases and the anti-virus engine are downloaded; other components of Dr.Web are not updated.

Creating update mirror

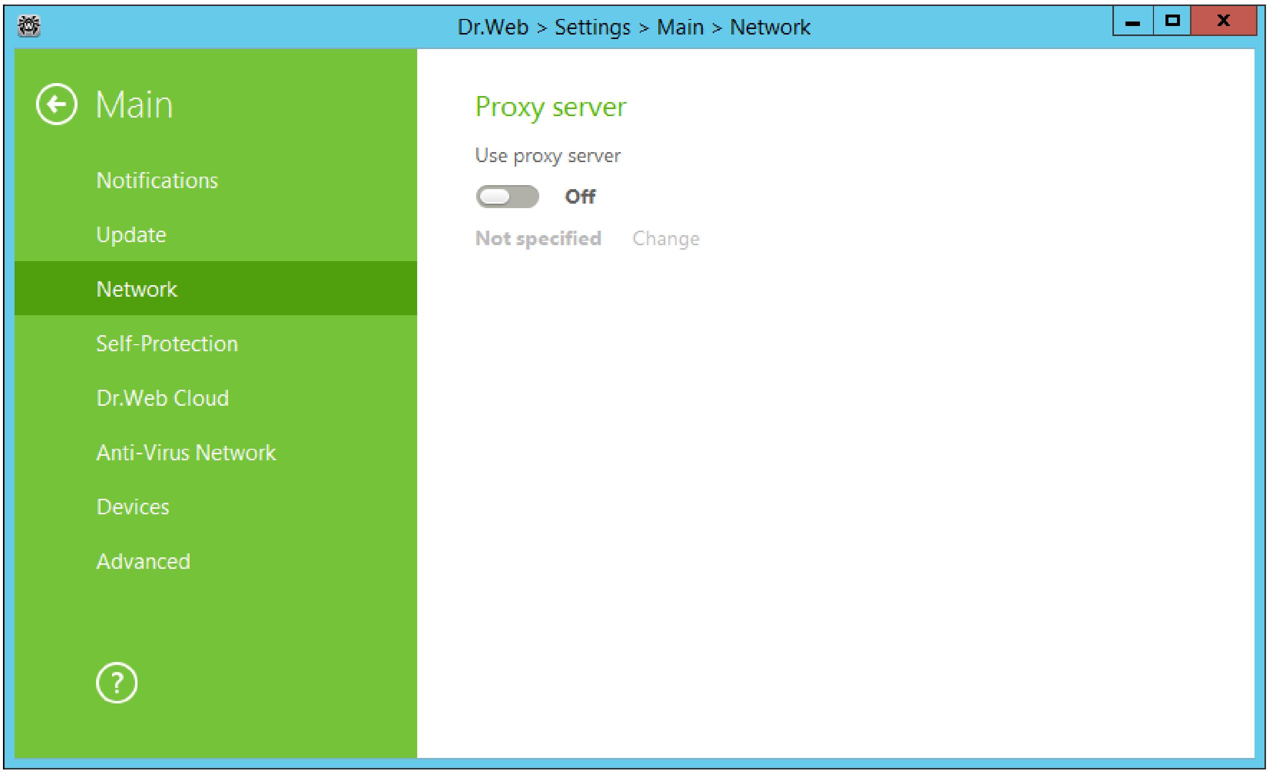
To allow other local network computers with installed Dr.Web products to use your computer as an update source, open **Advanced settings** and enable the appropriate option. Click **Edit** to specify the path to the folder where updates will be copied. If your computer is connected to several subnets, you can specify the IP address available to computers of only one subnet. You can also specify the port for HTTP connections.

10.3 Network

Proxy server

By default, all components use direct connection mode. If necessary, you can enable use of a proxy server and specify its connection settings. Click **Edit** to specify the following proxy server parameters:

Option	Description
Address	Specify the address of the proxy server.
Port	Specify the port of the proxy server.
Login	Specify the username to use when connecting to the proxy server.
Password	Specify the password to use when connecting to the proxy server under the provided username.
Authorization type	Select an authorization type required to connect to the proxy server.



Proxy server

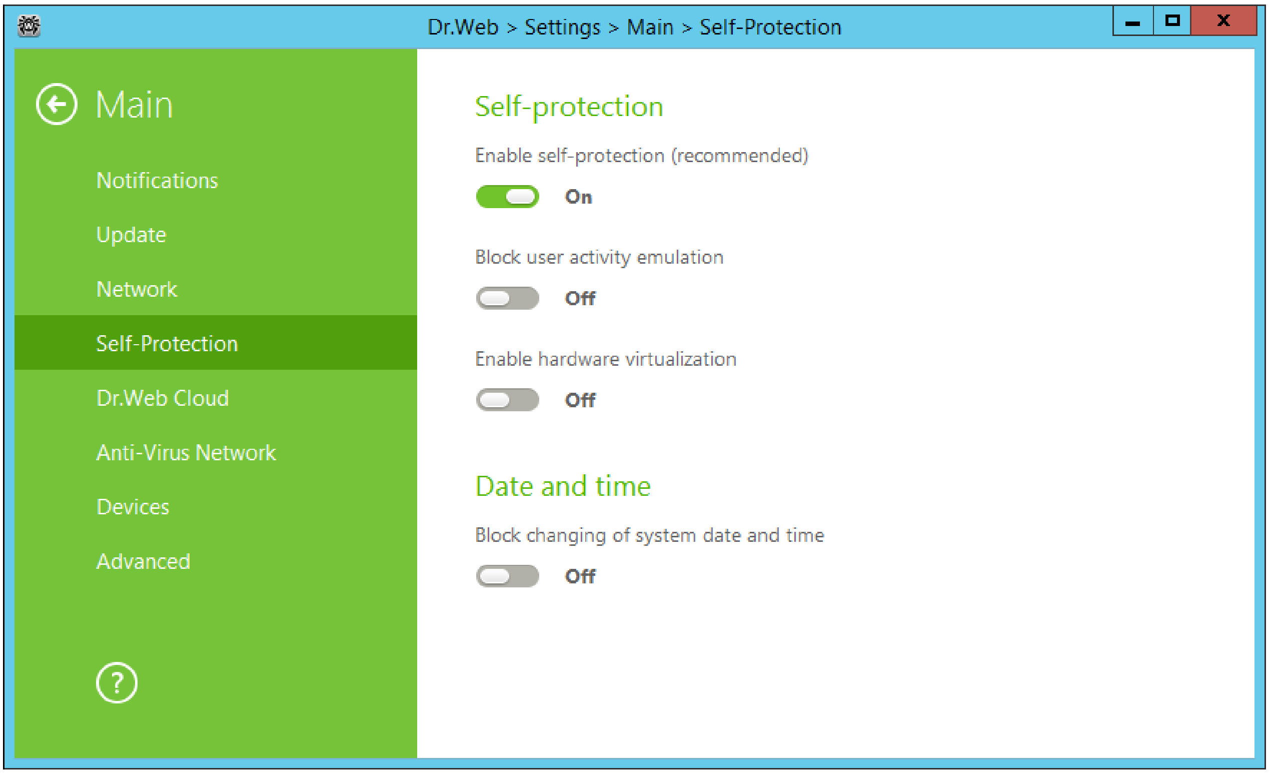
Use proxy server

Off

Not specified Change

10.4 Self-Protection

On this page, you can configure protection of Dr.Web itself from unauthorized modification by anti-antivirus programs or from accidental damage.



Self-protection

Enable self-protection (recommended)

On

Block user activity emulation

Off

Enable hardware virtualization

Off

Date and time

Block changing of system date and time

Off

Self-protection

The **Enable self-protection (recommended)** option allows to protect Dr.Web files and processes from unauthorized access. It is not recommended to disable Self-protection.

> ⚠ If any problems occur during operation of defragmentation programs, disable self-protection temporary.
>
> To rollback to a system restore point, disable self-protection.

The **Block user activity emulation** option allows to prevent any automatic changes in Dr.Web settings, including execution of scripts that emulate user interaction with Dr.Web and are launched by the user (for example, scripts to make changes in Dr.Web settings, license removal and other actions aimed at changing Dr.Web operation).

The **Use hardware virtualization** option allows to take full advantage of computer resources, which makes detection and curing of threats easier and enhances self-protection of Dr.Web. To enable this option, restart the computer.

Hardware virtualization works only if your computer's hardware and operating system support hardware virtualization.

Enabling this option may cause a conflict with some third-party software.

If problems occur, disable this option.

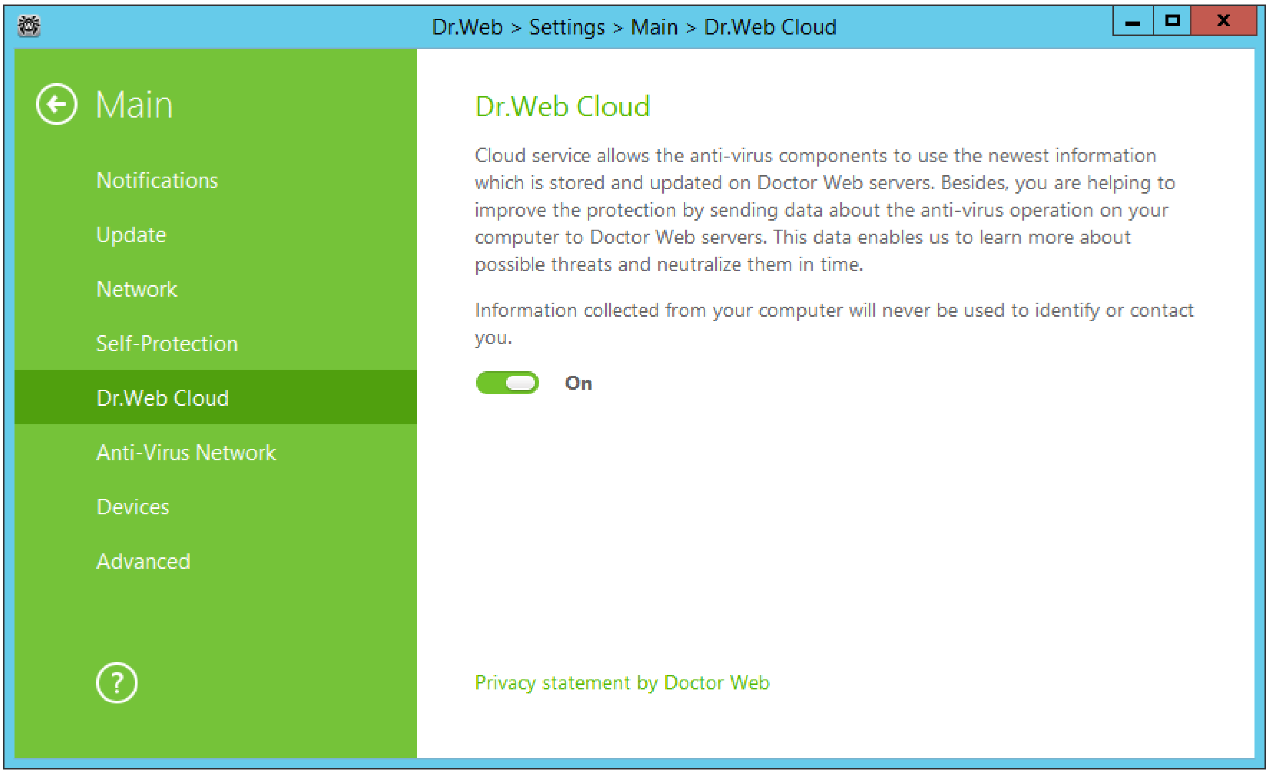
32-bit platforms do not support hardware virtualization

Date and time

The **Block changing of system date and time** option allows to prevent manual and automatic changes of the system date and time as well as of the time zone. This restriction is set for all system users. You can configure notification parameters to be informed on an attempt to change the system time.

10.5 Dr.Web Cloud

On this page, you can connect to Doctor Web cloud services and take part in Dr.Web quality improvement program.



Dr.Web Cloud

Cloud service allows the anti-virus components to use the newest information which is stored and updated on Doctor Web servers. Besides, you are helping to improve the protection by sending data about the anti-virus operation on your computer to Doctor Web servers. This data enables us to learn more about possible threats and neutralize them in time.

Information collected from your computer will never be used to identify or contact you.

On

Privacy statement by Doctor Web

Cloud services

Dr.Web Cloud provides most recent information on threats which is updated on Doctor Web servers in real-time mode and is used for anti-virus protection.

Depending on update settings, information on threats used by anti-virus components may become out of date. Cloud services can reliably protect your system from infected files.

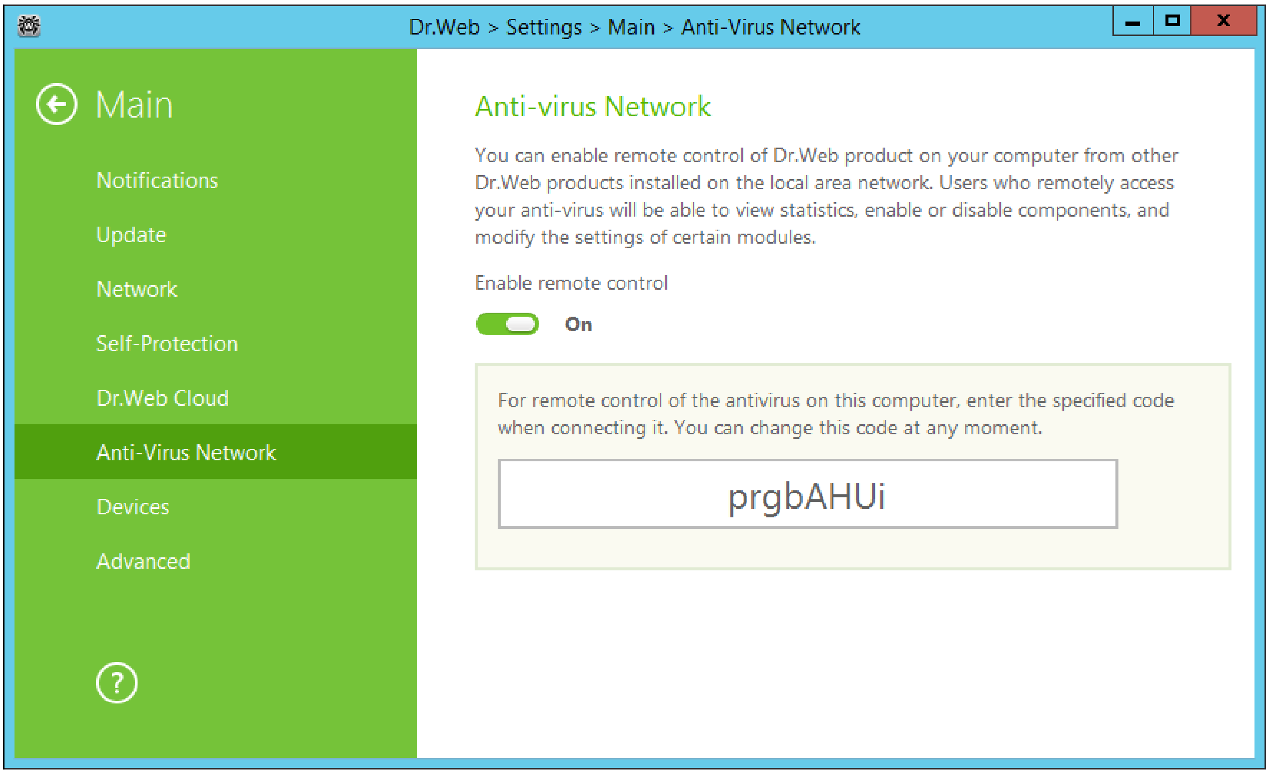
Software quality improvement program

If you participate in the software quality improvement program, impersonal data about Dr.Web operation on your computer will be periodically sent to Doctor Web servers. Received information is not used to identify or contact you.

Click the **Privacy policy by Doctor Web** link to look through a privacy statement on the Doctor Web official website.

10.6 Anti-virus Network

On this page, you can enable remote control of your anti-virus from other local network computers by Anti-Virus Network. If your computer is connected to an anti-virus network, you can control anti-virus protection state remotely (view statistics, enable or disable Dr.Web components and adjust their settings) and download updates from a local network computer. To allow local network computers with installed Dr.Web products to use a computer as an update source, configure an Update mirror on it.



Anti-virus Network

You can enable remote control of Dr.Web product on your computer from other Dr.Web products installed on the local area network. Users who remotely access your anti-virus will be able to view statistics, enable or disable components, and modify the settings of certain modules.

Enable remote control

On

For remote control of the antivirus on this computer, enter the specified code when connecting it. You can change this code at any moment.

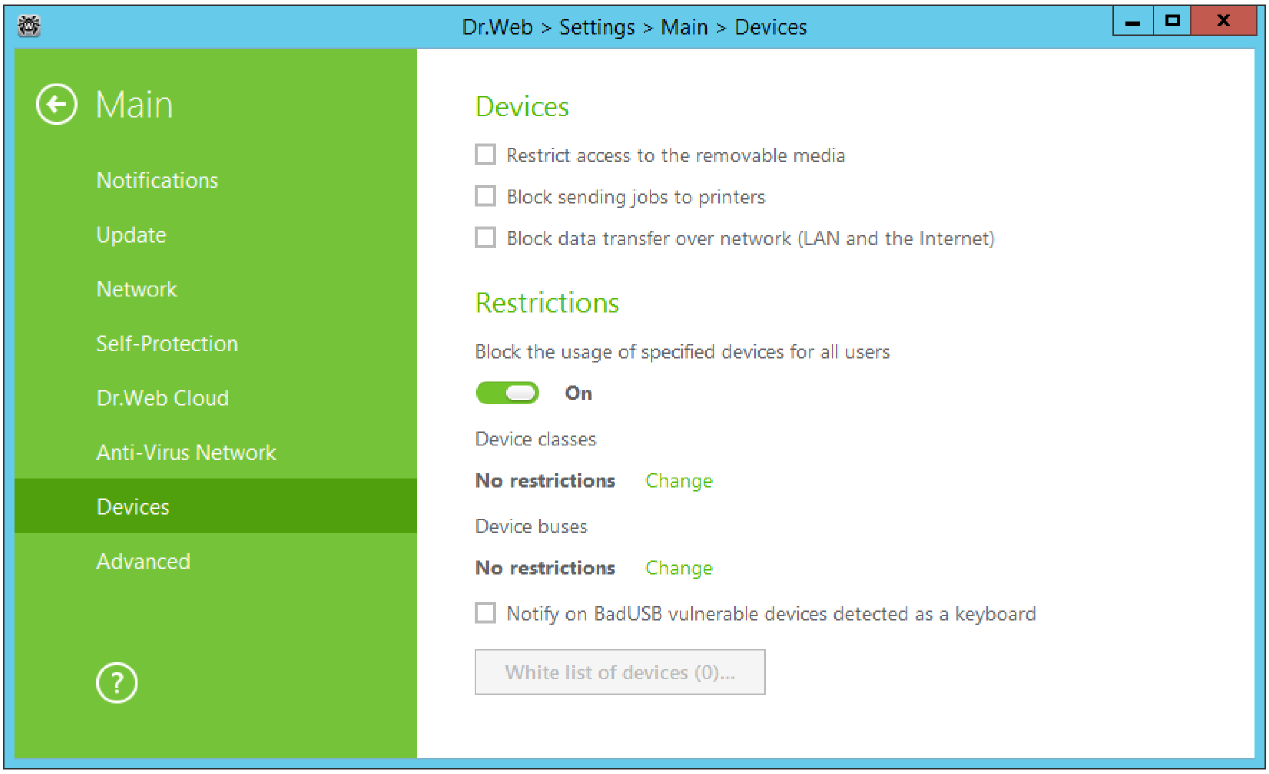
prgbAHUi

For remote access to Dr.Web settings on your computer, the password is required. You may use the password that is automatically generated when the option is enabled or set a new one.

Remote control allows you to view statistics, enable or disable components and modify their settings. Quarantine Manager and Scanner are not available. Dr.Web Firewall settings and statistics are not available either, but it is allowed to enable or disable the component.

10.7 Devices

Access control configurations are applied to all Windows accounts.



Dr.Web > Settings > Main > Devices

Devices

□ Restrict access to the removable media

□ Block sending jobs to printers

□ Block data transfer over network (LAN and the Internet)

Restrictions

Block the usage of specified devices for all users

On

Device classes

No restrictions Change

Device buses

No restrictions Change

□ Notify on BadUSB vulnerable devices detected as a keyboard

White list of devices (0)...

Devices

To block access to data on removable media (USB flash, floppy, CD/DVD, ZIP drives, etc.), enable the appropriate option. To block sending jobs to printers, enable the **Block sending jobs to printers** option. This option is disabled by default. You can also block data transfer over network (LAN and the Internet).

Infected USB devices can be identified by your computer as a keyboard. If you want Dr.Web to check whether the connected USB device is a keyboard, enable the **Notify on BadUSB vulnerable devices detected as a keyboard** option.

Device and bus classes

To block access to specified device or bus classes, enable the appropriate option. Click the **Edit** button to make a list of such objects. In the open window, select device or bus classes that you want to restrict access to. Click **OK** to save the changes. To close the window without saving the changes, click **Undo**.

White list of devices

After you restricted access to some device or bus classes, you can allow access to certain devices by adding them to the white list. You can also add a certain device to the white list if you do not want it to be checked for BadUSB vulnerability.

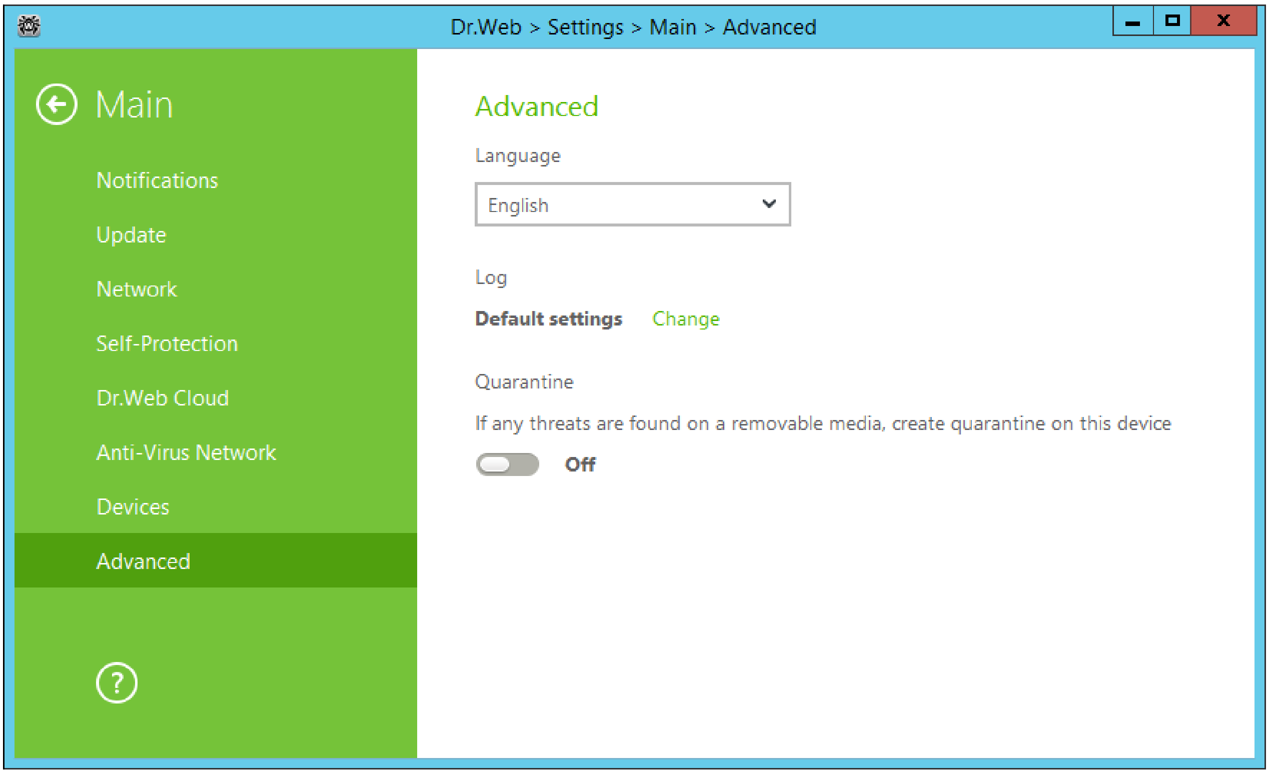
To add a device to the white list, do the following:

1. Click **White list of devices** (the button becomes available if restrictions are set).
2. Make sure that the device is connected to the computer.
3. Click ⊕. In the open window, click **Browse** and select the device. You can use a filter to view only connected or only disconnected devices. Click **OK**.
4. You can configure access rules for devices with file systems. For that, from the **Rule** column, select one of the following modes: **Allow all** or **Read-only**. To add a new rule for a specific user, click ⊕. To delete a rule, click 🗑.
5. To save the changes, click **OK**. To close the window without saving the changes, click **Undo**. The white list of devices opens.
6. To edit a rule set, select it from the list and click ✎.
7. To remove a rule set, select it from the list and click 🗑.

10.8 Advanced

On this page, you can select a language for the settings, configure logging options and Quarantine settings.

To set another program language, select it from the corresponding drop-down list. New languages are automatically added to the list. Thus, it contains all localization languages that are currently available for theDr.Web graphical interface.



Dr.Web > Settings > Main > Advanced

Advanced

Language

English

Log

Default settings Change

Quarantine

If any threats are found on a removable media, create quarantine on this device

Off

Log settings

To configure log settings, click the corresponding **Edit** button.

> Size of a log file is restricted to 10 MB by default (and 100 MB for SpIDer Guard). If the log file size exceeds the limit, the content is reduced to:
>
> - Specified size if the current session information does not exceed the limit.
> - Size of the current session if the session information exceeds the limit.

By default, the standard logging mode is enabled for all the Dr.Web components and the following information is logged:

Component	**Information**
SpIDer Guard	Time of updates and SpIDer Guard starts and stops, virus events, names of scanned files, names of packers, and contents of scanned complex objects (archives, email attachments, file containers). It is recommended to use this mode to determine the most frequent objects scanned by SpIDer Guard. If necessary, you can add these objects to the list of exclusions in order to increase computer performance.
Scanner	In this mode, main events are logged, such as time of updates, time of Dr.Web Scanner starts and stops, information on detected threats, names of packers, and content of scanned archives.

Component	Information
Update Dr.Web	List of updated Dr.Web files and their download status, date and time of updates, and details on auxiliary script execution and Dr.Web component restart.
Dr.Web Services	Information on Dr.Web components, changes in their settings, component starts and stops, preventive protection events, connections to anti-virus network.

Memory dump creation

The **Create memory dumps at scan errors** option allows to save useful information on operation of several Dr.Web components. This helps Doctor Web technical support specialists analyze an occurred problem in detail and find a solution. It is recommended to enable this option on request of Doctor Web technical support specialists or when errors of scanning or neutralizing occur. Memory dump is saved to a .dmp file located in the folder %PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\.

Enabling detailed logging

> ⚠ Upon logging detailed data on Dr.Web operation, the maximum amount of information is recorded. This will result in disabling of log file size limitations and will have an impact on system and Dr.Web performance. It is recommended to use this mode only when errors occur in component operation or by request of Doctor Web technical support.

1. To enable detailed logging for a Dr.Web component, select the corresponding check box.
2. By default, detailed logging is enabled until the first restart of the operating system. If it is necessary to log component activity before and after the restart, select the **Continue detailed logging after restart (use only by request of Doctor Web technical support)** check box.
3. Save the changes.

Quarantine settings

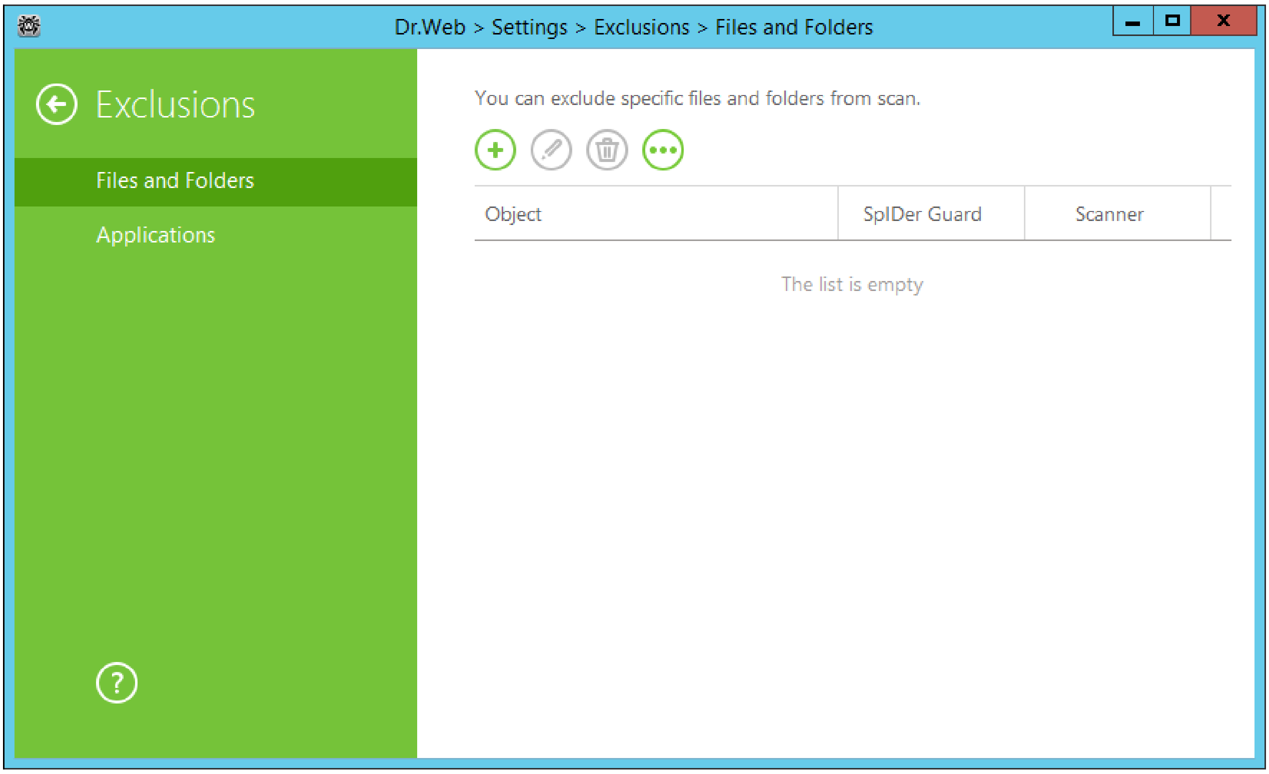
You can select the isolation mode for infected objects detected on portable data carriers. When this option is enabled, detected threats are moved to the folder on this data carrier without being encrypted. The Quarantine folder is created on portable data carriers only when they are accessible for writing. The use of separate folders and omission of encryption on portable data carriers prevents possible data loss. If the option is enabled, the detected threat is moved to Quarantine on the local disc.

11. Exclusions

11.1 Files and Folders

In this section, you can manage the list of files and folders to be excluded from scanning by SpIDer Guard and Scanner. You can exclude the anti-virus quarantine folders, working folders of some programs, temporary files (paging file), and so on.

The default list is empty. Add particular files and folders to exclusions or use masks to disable scanning of a certain group of files. Any added object can be excluded from the scanning of both components or from scanning of each component separately.



You can exclude specific files and folders from scan.

Object	SpIDer Guard	Scanner

The list is empty

To configure list of exclusions

1. To add a file or folder to the exclusion list, do one of the following:
   - To add an existing file or folder, click ⊕. In the open window, click **Browse** and select the item in the standard dialog window. You can enter the full path to the file or folder or edit the path in the field before adding it to the list.
   - To exclude a file with a particular name, enter the name and the extension without the path;
   - To exclude a group of files or folders, enter the mask of their names.
2. In the configuration window, specify the components that must not scan this file.
3. Click **OK**. The file or folder will appear on the list.

4. To edit an existing exclusion, select the corresponding item from the list and click ✎.
5. To list other files and folders, repeat steps 1 to 2. To remove a file or folder from the list, select the corresponding item and click 🗑.

A mask denotes the common part of object names, at that:

- The asterisk (*) character replaces any, possibly empty, sequence of characters.
- The question mark (?) replaces any character (one).
- Other mask characters do not replace anything and mean that in this place the name must contain this particular character.

Examples:

- file.txt—excludes all files with the name “file” and the .txt extension located in all folders.
- C:\folder\file.txt—excludes file.txt file stored in C:\folder.
- file*—excludes all files located in all folders without regard for the extension with the names starting with “file” .
- file.*—excludes all files with the name “file” and with all extensions located in all folders.
- file—excludes all files with the name “file” located in all folders without regard for the extension.
- C:\folder\ or C:\folder\**—excludes all files located in C:\folder and its subfolders.
- C:\folder\*—excludes all files located in C:\folder and its subfolders on any nesting level.
- C:\folder\*.txt—excludes all *.txt files stored in C:\folder. The *.txt files stored within subfolders will be scanned.
- C:\folder\**.txt—excludes all *.txt files stored in the first nesting level subfolders of C:\folder.
- C:\folder\***.txt—excludes all *.txt files stored in subfolders of any nesting level within C:\folder. The files stored in C:\folder itself, including *.txt files, will be still scanned.

Managing listed objects

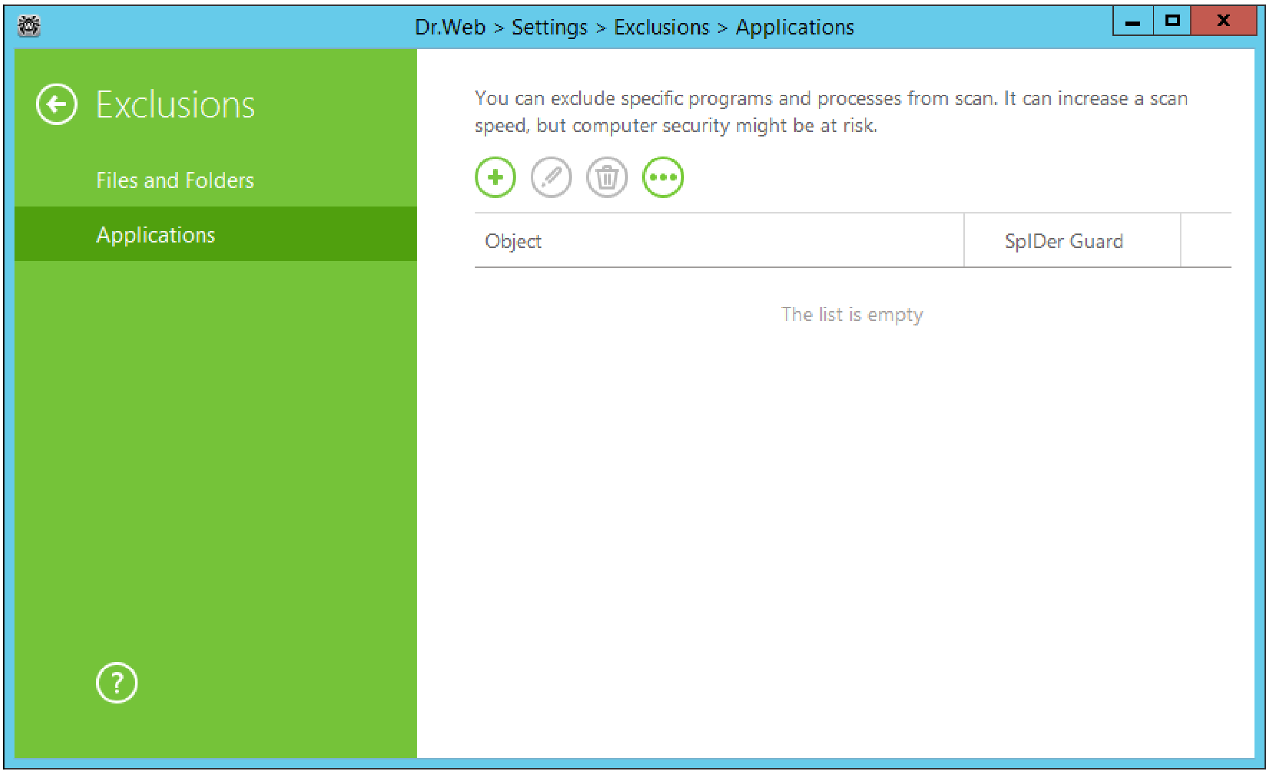
Click ⋯ to access the following options:

- **Export**—allows to save the created list of exclusions to be used on another computer where Dr.Web is installed.
- **Import**—allows to use the list of exclusions created on another computer.
- **Clear all**—allows to remove all objects from the list of exclusions.

11.2 Applications

You can specify a list of programs and processes to be excluded from scanning by SpIDer Guard.

By default, the list is empty.



Dr.Web > Settings > Exclusions > Applications

You can exclude specific programs and processes from scan. It can increase a scan speed, but computer security might be at risk.

Object	SpIDer Guard

The list is empty

To configure list of exclusions

1. To add a program or a process to the exclusion list, click ⊕. Do one of the following:
   - In the open window, click **Browse** and select an application in the standard dialog window. You can enter the full path to the application in the field manually.
   - To exclude an application from scanning, enter its name in the field. The full path to the application is not required (for example, `example.exe`);
   - To exclude applications, enter the mask of their names;
   - You can exclude an application from scanning by the name of a variable if the name and a value of this variable are specified in the system variable settings.
2. In the configuration window, specify that SpIDer Guard must not check the selected application.
3. Click **OK**. The selected application will appear on the list.
4. If necessary, repeat the procedure to add other programs.
5. To edit an existing exclusion, select the corresponding item from the list and click ✎.
6. To remove an application from the list, select the corresponding item and click 🗑.

A mask denotes the common part of object names, at that:

- The asterisk (*) character replaces any, possibly empty, sequence of characters.
- The question mark (?) replaces any character (one).

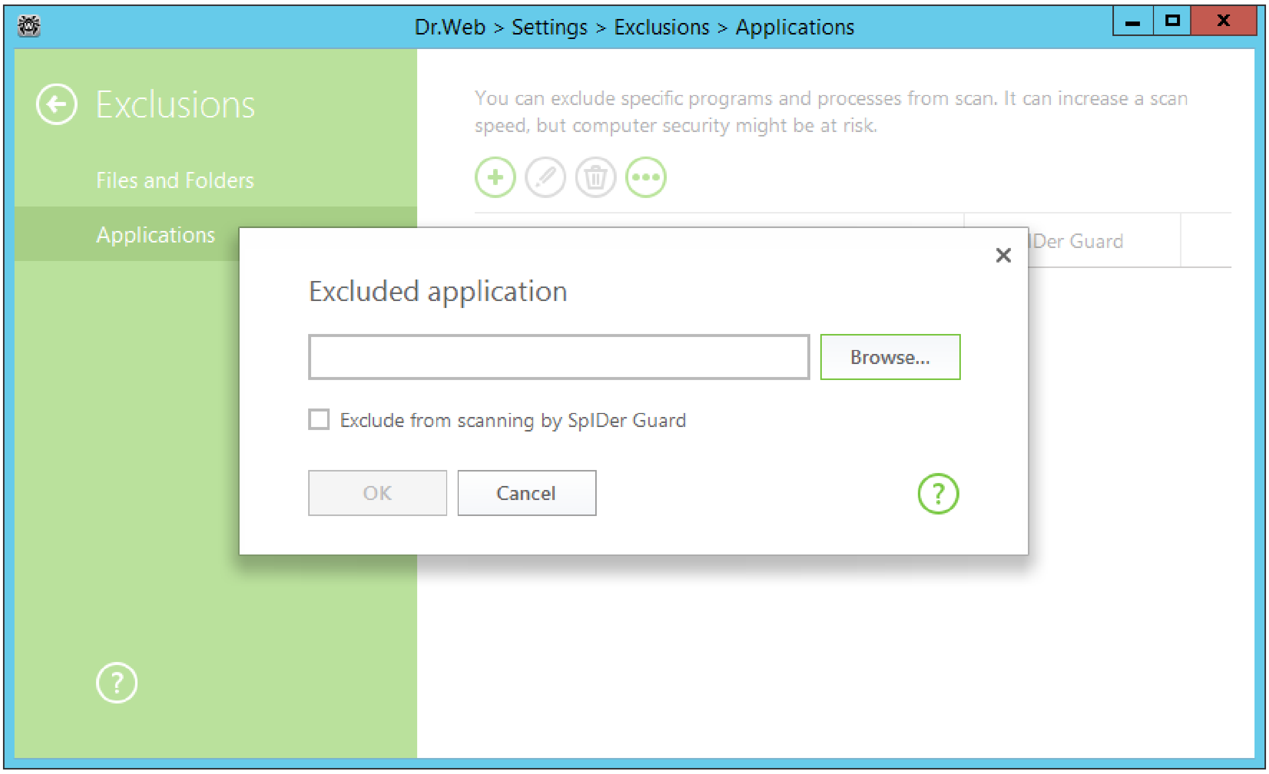
Examples:

- `C:\Program Files\folder\example.exe` – excludes the application example.exe in the folder C:\Program Files\folder from scanning.
- `C:\Program Files\folder\*.exe` – excludes applications in the folder C:\Program Files\folder from scanning. Applications in subfolders will be scanned.
- `C:\Program Files\*\*.exe` – excludes applications stored in the first nesting level subfolders of C:\Program Files.
- `C:\Program Files\**\*.exe` – excludes applications in subfolders of any nesting level located in the folder C:\Program Files from scanning. Applications in the folder C:\Program Files will be scanned.
- `C:\Program Files\folder\exam*.exe` – excludes any application in the folder C:\Program Files\folder from scanning if their names begin with “exam”. In subfolders, these applications will be scanned.
- `example.txt`—excludes all applications with the name “example” and the .exe extension located in all folders.
- `example*` —excludes all types of applications with the name starting with “example” located in all folders.
- `example.*` —excludes all applications with the name “example” in all folders without regard for the extension.
- `%EXAMPLE_PATH%\example.exe` – excludes an application by the name of a system variable. A name of a system variable and its value can be specified in the operating system settings.

  For Windows 7 and higher: **Control Panel** → **System** → **Advanced system settings** → **Advanced** → **Environment variables** → **System variables**.

  A name of a variable in an example: `EXAMPLE_PATH`.

  A value of a variable in an example: `C:\Program Files\folder`.



Dr.Web > Settings > Exclusions > Applications

Exclusions

Files and Folders

Applications

You can exclude specific programs and processes from scan. It can increase a scan speed, but computer security might be at risk.

Excluded application

Browse...

□ Exclude from scanning by SpIDer Guard

OK | Cancel

Managing listed objects

Click ⋯ to access the following options:

- **Export**—allows to save the created list of exclusions to be used on another computer where Dr.Web is installed.
- **Import**—allows to use the list of exclusions created on another computer.
- **Clear all**—allows to remove all objects from the list of exclusions.

12. Protection Components

12.1 SpIDer Guard

SpIDer Guard is an on-access anti-virus scanner that constantly resides in memory and scans files and RAM on the fly instantly detecting any malicious activity.

With the default settings, the component performs on-access scans of files that are being created or changed on the hard drives and all files that are opened on removable media. Moreover, SpIDer Guard constantly monitors running processes for virus-like activity and, if such is detected, blocks malicious processes and reports on the event. On detection of an infected object, SpIDer Guard processes it according to the specified settings.

Files within archives and mailboxes are not scanned. If a file within an archive or email attachment is infected, the malicious object will be detected and neutralized by SpIDer Guard immediately after you try to extract the archived files or download the attachment.

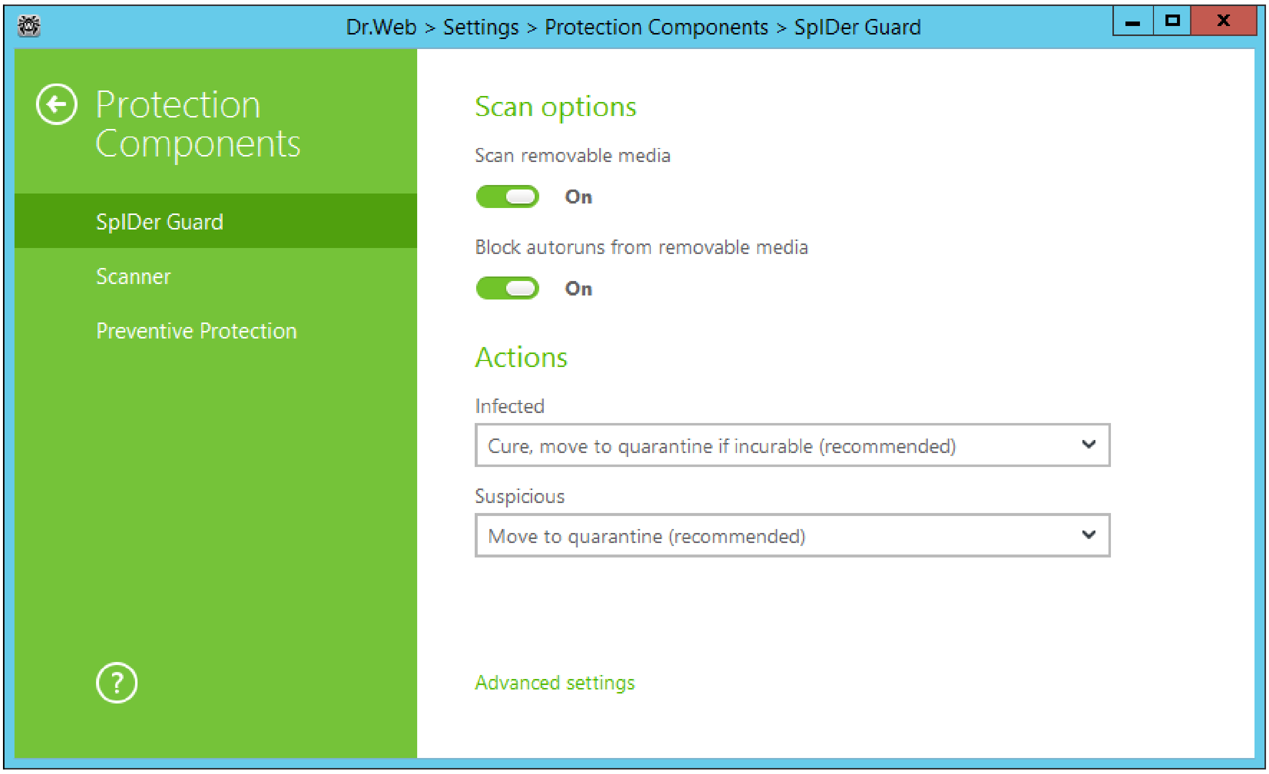
On detection of an infected object, SpIDer Guard applies actions to it according to the specified settings. You can change settings to configure automatic reaction to different virus events.

By default, SpIDer Guard loads automatically when Windows starts and cannot be unloaded during the current Windows session.

12.1.1 Configuring SpIDer Guard

To access the SpIDer Guard settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the Settings window.

The default settings are optimal for most cases. Do not change them unnecessarily.



Dr.Web > Settings > Protection Components > SpIDer Guard

Scan options

Scan removable media: On

Block autoruns from removable media: On

Actions

Infected: Cure, move to quarantine if incurable (recommended)

Suspicious: Move to quarantine (recommended)

Scan options

By default SpIDer Guard checks objects on removable media such as CD/DVD, flash memory, and so on. This option helps to protect your computer from viruses transmitted via removable media.

> ⚠ If any problem occurs during installation with the autorun option, it is recommended to temporary disable the **Block autoruns from removable media** option.

Actions

On this page, you can configure reactions of SpIDer Guard to detection of infected or suspicious files and malware.

For different types of compromised objects, actions are assigned separately from the respective drop-down lists:

- **Infected**—objects infected with a known and (supposedly) curable virus.
- **Suspicious**—objects supposedly infected with a virus or containing a malicious object.
- Various potentially dangerous objects (riskware). To expand the entire list of objects, click the **Advanced settings** link.

Reaction of SpIDer Guard to detection of various malicious software is also set separately. Set of actions available for the selection depends on the type of the virus event.

By default, SpIDer Guard attempts to cure infected and supposedly curable files, moves other most dangerous objects to Quarantine, and ignores minor threats such as jokes, hacktools, and riskware. The reactions of SpIDer Guard are similar to those of Dr.Web Scanner.

You can select one of the following actions for detected threats:

Action	Description
Cure, move to quarantine if not cured	Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
Cure, delete if not cured	Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
Delete	Instructs to delete the object. This action is not available for boot sectors.
Move to Quarantine	Instructs to move the object to a specific folder of Quarantine. This action is not available for boot sectors.
Ignore	Instructs to skip the object without performing any action or displaying a notification. The action is available only for potentially dangerous files (adware, dialers, jokes, hacktools, and riskware).

SpIDer Guard does not check complex objects such as archives, mailboxes, or file containers. No action is performed on such objects or on files within them.

Copies of all processed objects are stored in Quarantine.

Scan mode

In this group, you can set up what actions with objects require scanning “on-the-fly” with SpIDer Guard.

Option	Description
Optimal (recommended)	This scan mode is used by default. In this mode, SpIDer Guard scans objects only when one of the following actions is traced: • For objects on hard drives, an attempt to execute a file, create a new file, or add a record to an existing file or boot sector. • For objects on removable media, an attempt to access file or boot sectors in any way (write, read, execute).
Paranoid	In this mode, SpIDer Guard scans files and boot sectors on hard or network drives and removable media at any attempt to access them (create, write, read, execute).

⚠ When running in the Optimal mode, SpIDer Guard does not terminate execution of an EICAR test file and the file is not processed as malicious since it does not pose any actual threat to your system. However, if you copy or create such a file in your system, it will be detected by SpIDer Guard and moved to Quarantine by default.

The **Optimal** mode is recommended to use after a thorough scan of all hard drives by Dr.Web Scanner. With this mode activated, SpIDer Guard prevents penetration of new viruses and other malicious objects via removable media into your computer while preserving performance by omitting knowingly "clean" objects from repeated scans.

The **Paranoid** mode ensures maximum protection but considerably reduces computer performance.

In any mode, objects on removable media and network drives are scanned only if the corresponding options in the **Scan options** group are enabled.

⚠ Operating system may register some removable media as hard drives (for example, portable USB hard drives). Scan such devices with Dr.Web Scanner when you connect them to the computer.

By default, files within archives and mailboxes are not scanned. This does not affect security of your computer when it is constantly protected by SpIDer Guard, only delays the moment of detection. If a file within an archive or email attachment is infected, the malicious object will be detected and neutralized by SpIDer Guard immediately when you try to extract the archived files or download the attachment.

Advanced settings

The settings of this group allow to specify parameters for scanning objects on-the-fly and are always applied regardless of the selected SpIDer Guard operation mode. You can enable:

- Use of heuristic analysis;

- scan of programs and modules to download;
- scan of installation packages;
- scan of files on network drives (not recommended);
- scan of a computer for the presence of rootkits (recommended).

Heuristic analysis

By default, SpIDer Guard performs scan using heuristic analysis. If this option is disabled, SpIDer Guard will use signature analysis only.

Background rootkit scanning

Anti-rootkit component included in Dr.Web provides options for background scanning of the operating system for complex threats and curing of detected active infections when necessary. This option is enabled by default.

If this option is enabled, Dr.Web Anti-rootkit constantly resides in memory. In contrast to the on-the-fly scanning of files by SpIDer Guard, scanning for rootkits includes checking of autorun objects, running processes and modules, Random Access Memory (RAM), MBR/VBR disks, computer BIOS system, and other system objects.

One of the key features of Dr.Web Anti-rootkit is delicate attitude towards consumption of system resources (processor time, free RAM, and others) as well as consideration of hardware capacity.

When Dr.Web Anti-rootkit detects a threat, it notifies you on the detection and neutralizes the malicious activity.

> During background rootkit scanning, files and folders specified on the Excluded files page are excluded from scanning.

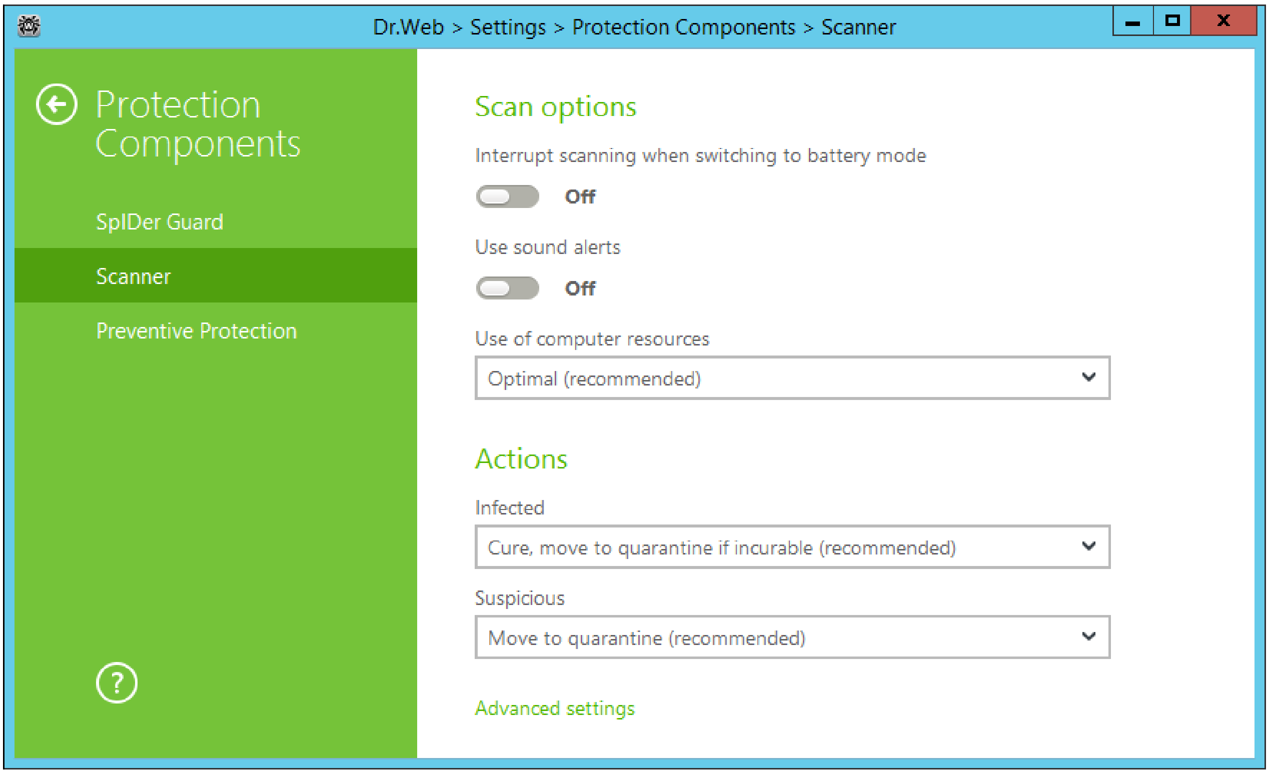
Background rootkit scanning is enabled by default.

> Disabling of SpIDer Guard does not affect background scanning. If the option is enabled, background scanning is performed regardless of whether SpIDer Guard is running or not.

12.2 Scanner

> To access the Scanner settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the Settings window.

The default settings are optimal for most cases. Do not change them unnecessarily.



Dr.Web > Settings > Protection Components > Scanner

Scan options

Interrupt scanning when switching to battery mode

Off

Use sound alerts

Off

Use of computer resources

Optimal (recommended)

Actions

Infected

Cure, move to quarantine if incurable (recommended)

Suspicious

Move to quarantine (recommended)

Advanced settings

Scan options

In this group, you can configure general parameters of Dr.Web Scanner operation.

- **Interrupt scanning when switching to battery mode**. Enable this option to interrupt scanning when switching to battery mode. Option is disabled by default.
- **Use sound alerts**. Enable this option for Dr.Web Scanner to use sound alerts for every event. Option is disabled by default.
- **Use of computer resources**. This option limits the use of computer resources by Dr.Web Scanner. The default value is optimal for most cases.

Actions

On this page, you can configure reaction of Scanner on detection of infected or suspicious files and archives or other malicious objects.

For different types of compromised objects, actions are assigned separately from the respective drop-down lists:

- **Infected**—objects infected with a known and (supposedly) curable virus.
- **Suspicious**—objects supposedly infected with a virus or containing a malicious object.
- Objects that pose potential threat (riskware).

Reaction of Scanner to detection of various malicious software is also set separately. Set of actions available for the selection depends on the threat type.

By default, Scanner attempts to cure the infected and supposedly curable files, moves other most dangerous objects to Quarantine.

You can select one of the following actions for detected threats:

Action	Description
Cure, move to quarantine if not cured	Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
Cure, delete if not cured	Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
Delete	Instructs to delete the object. This action is not available for boot sectors.
Move to Quarantine	Instructs to move the object to a specific folder of Quarantine. This action is not available for boot sectors.
Ignore	Instructs to skip the object without performing any action or displaying a notification. The action is available only for potentially dangerous files (adware, dialers, jokes, hacktools, and riskware).

Threats within complex objects cannot be processed individually. For such threats, Dr.Web Scanner applies an action selected for this type of a complex object.

Additional tasks

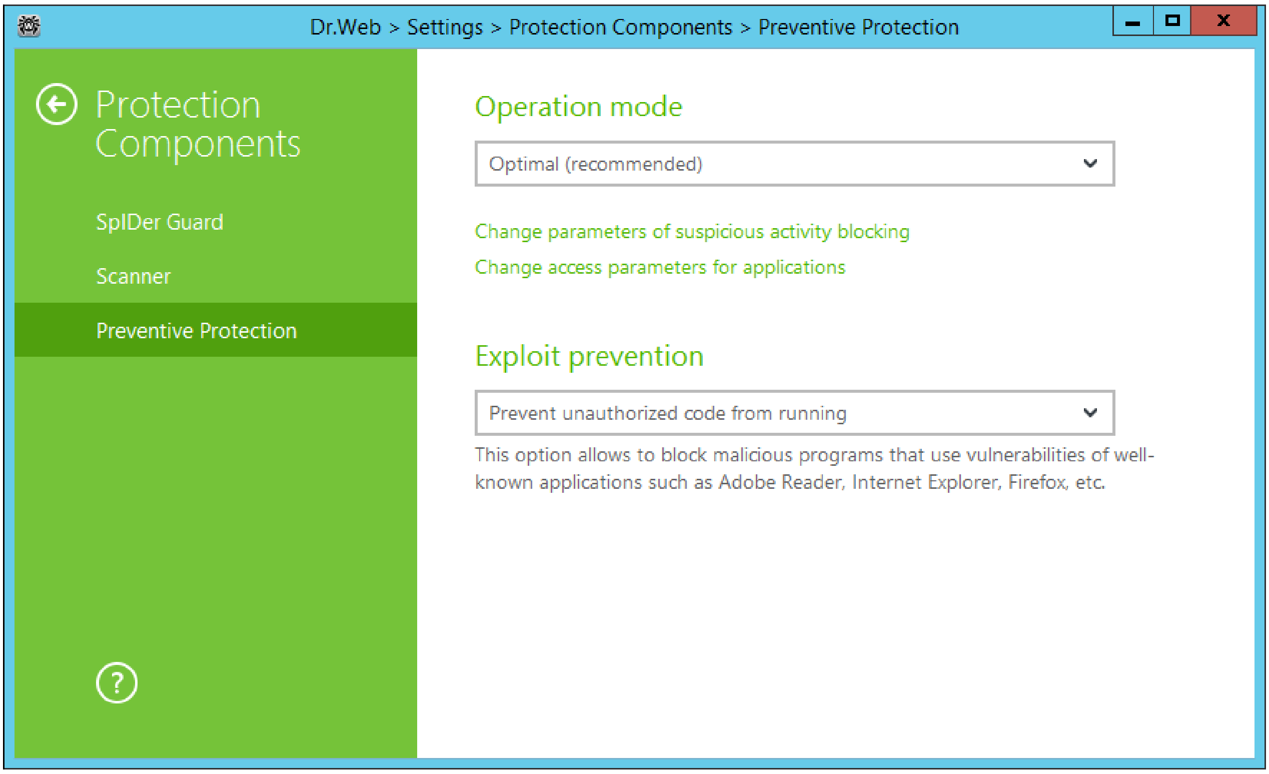
You can disable check of installation packages, archives, and email files. This option is enabled by default.

You can also select one of the following actions for Scanner to perform once scanning is complete:

1. **Do not apply action**. Scanner will display the list of detected threats.
2. **Neutralize detected threats**. Scanner will neutralize threats automatically.
3. **Neutralize detected threats and shut down computer**. Scanner will shut down the computer once threats are automatically neutralized.

12.3 Preventive Protection

On this page, you can configure Dr.Web reaction to such actions of other programs that can compromise security of your computer and select protection level against exploits.


Dr.Web > Settings > Protection Components > Preventive Protection
Protection Components
SpIDer Guard
Scanner
Preventive Protection
Change parameters of suspicious activity blocking
Change access parameters for applications

Operation mode

Optimal (recommended)

Exploit prevention

Prevent unauthorized code from running

This option allows to block malicious programs that use vulnerabilities of well-known applications such as Adobe Reader, Internet Explorer, Firefox, etc.

At that, you can configure a separate protection mode for particular applications or configure a general mode whose settings will apply to all other processes.

To configure the general mode, select it from the **Operation mode** list or click **Change parameters of suspicious activity blocking**. As a result of the second action, a window opens providing you with details on each mode and editing options. All changes are saved in the User mode. In this window, you can also create a new profile for saving necessary settings.

To create a new profile

1. Click ⊕.
2. In the open window, enter a name for the new profile.
3. Look through default settings and, if necessary, edit them.

To configure preventive protection settings for particular applications, click **Change access parameters for applications**. In the open window, you can add a new rule or edit or delete an existing rule.

To add a rule

1. Click ⊕.
2. In the open window, click **Browse** and specify the path to the application executable file.
3. Look through default settings and, if necessary, edit them.

To edit an existing rule, select it from the list and click ✎.

To delete an existing rule, select it from the list and click 🗑.

For more information about settings of each operation mode, refer to the Preventive Protection Level section.

Preventive protection level

In the **Optimal** mode which is set by default, Dr.Web disables automatic changes of system objects, whose modification explicitly signifies a malicious attempt to harm the operating system. It also blocks low-level access to disk and protects the HOSTS file from modification.

If there is a high risk of your computer getting infected, you can increase protection by selecting the **Medium**. In this mode, access to the critical objects, which can be potentially used by malicious software, is blocked.

> ⚠ Using this mode may lead to compatibility problems with legitimate software that uses the protected registry branches.

When required to have total control of access to critical Windows objects, you can select the **Paranoid**. In this mode, Dr.Web also provides you with interactive control over loading of drivers and automatic running of programs.

With the **User-defined** mode, you can set a custom protection level for various objects.

Protected object	**Description**
Integrity of running applications	This option allows detection of processes that inject their code into running applications. It indicates that the process may compromise computer security. Processes that are added to the Exclusions are not monitored.
Integrity of user files	This option allows detection of processes that modify user files with the known algorithm, which indicates that the process may compromise computer security. Processes that are added to the Exclusions are not monitored. To protect your data from modification, you can enable creation of protected copies that contain important data.

Protected object	**Description**
HOSTS file	The operating system uses the HOSTS file when connecting to the Internet. Changes to this file may indicate virus infection.
Low level disk access	Block applications from writing on disks by sectors while avoiding the file system.
Drivers loading	Block applications from loading new or unknown drivers.
Critical Windows objects	Other options allow protection of the following registry branches from modification (in the system profile as well as in all user profiles). Image File Execution Options: • Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options User Drivers: • Software\Microsoft\Windows NT\CurrentVersion\Drivers32 • Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers Winlogon registry keys: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Winlogon notifiers: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify Windows registry startup keys: • Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib Executable file associations: • Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys) • Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys) Software Restriction Policies (SRP): • Software\Policies\Microsoft\Windows\Safer Browser Helper Objects for Internet Explorer (BHO): • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Autorun of programs: • Software\Microsoft\Windows\CurrentVersion\Run • Software\Microsoft\Windows\CurrentVersion\RunOnce • Software\Microsoft\Windows\CurrentVersion\RunOnceEx • Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup

Protected object	Description
	• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup • Software\Microsoft\Windows\CurrentVersion\RunServices • Software\Microsoft\Windows\CurrentVersion\RunServicesOnce Autorun of policies: • Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Safe mode configuration: • SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal • SYSTEM\ControlSetXXX\Control\SafeBoot\Network Session Manager parameters: • System\ControlSetXXX\Control\Session Manager\SubSystems, Windows System services: • System\CurrentControlXXX\Services

If any problems occur during installation of important Microsoft updates or installation and operation of programs (including defragmentation programs), temporarily disable Preventive Protection.

If necessary, you can configure desktop and email notifications on Preventive Protection actions.

Exploit prevention

This option allows to block malicious programs that use vulnerabilities of well-known applications. From the corresponding drop-down list, select the required level of protection.

Protection level	Description
Prevent unauthorized code from being executed	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, it will be blocked automatically.
Interactive mode	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, Dr.Web will display an appropriate message. Read the information and select a suitable action.
Allow unauthorized code to be executed	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, it will be allowed automatically.

13. Statistics

To view statistics on the components operation, open the SpIDer Agent menu, go to **Statistics**. On the **Statistics** page, reports for the following groups are available:

- Threats
- Update

A detailed report is available for the **Threats** and **Update** groups. You can also apply filters to these reports.

Detailed report

To view a detailed report about Dr.Web operation events, choose a necessary event and click ⓘ. Click the button again to hide the detailed report.

Click ⋯ to remove, copy, export selected events or a report file, or clear a report.

You can use filters to select a certain event.

Filters

To view a list of only those events that correspond to specific parameters, use filters. All the reports have preset filters that are available in a drop-down list on the top of a page.

You can create custom event filters. To create a new filter, click ▽, select **Create** in a drop-down list. and then specify necessary filtering criteria. In the **Component** field, you can specify several components at once.

Events can be filtered by codes. To do this, specify them in the **Code (Example: 100-103, -102, 403)** field according to the following rules:

- Codes can be separated by commas
- You can specify a range of necessary codes (for example, 100-103).
- A code can be excluded from the range by using the - symbol

Therefore, "`100-103,-102,403`" means to show all events from 100 to 103, exclude the "-102" code from filtering and show the event "403".

All created filters can be edited or removed.

Appendices

Appendix A. Command-Line Parameters

Additional command-line parameters (switches) are used to set parameters for programs, which can be launched by opening an executable file. This relates to Dr.Web Scanner, Console Scanner and Dr.Web Updater. The switches can set parameters that are either not present in the configuration file or have a higher priority than those specified in the file.

Switches begin with the forward slash (/) character and are separated by spaces as other command-line parameters.

The switches are listed alphabetically.

Scanner and Console Scanner Parameters

`/AA`—apply actions to detected threats automatically. (For Scanner only.)

`/AC`—scan installation packages. Option is enabled by default.

`/AFS`—use forward slash to separate paths in an archive. Option is disabled by default.

`/AR`—scan archives. Option is enabled by default.

`/ARC:`<*compression_ratio*>—maximum compression level. If the compression ratio of the archive exceeds the limit, Scanner neither unpacks nor scans the archive. By default: unlimited.

`/ARL:`<*nesting_level*>—maximum archive nesting level. By default: unlimited.

`/ARS:`<*size*>—maximum archive size (in KB). By default: unlimited.

`/ART:`<*size*>—minimum size of a file inside an archive beginning from which compression ratio check is performed (in KB). By default: unlimited.

`/ARX:`<*size*>—maximum size of a file inside an archive that is scanned (in KB). By default: unlimited.

`/BI`—show information on virus databases. Option is enabled by default.

`/CUSTOM`—perform a custom scan. If additional parameters are set (for example, objects to be scanned or /TM and /TB parameters), only the specified objects will be scanned. (For Scanner only.)

`/CL`—use Dr.Web cloud service. Option is enabled by default. (For Console Scanner only.)

`/DCT`—do not display estimated scan time. (For Console Scanner only.)

/DR—scan folders recursively (scan subfolders). Option is enabled by default.

/E:<*number_of_threads*>—perform scanning in specified number of threads.

/FAST—perform an express scan of the system. If additional parameters are set (for example, objects to be scanned or /TM and /TB parameters), the specified objects will also be scanned. (For Scanner only.)

/FL:<*file_name*>—scan paths listed in the specified file.

/FM:<*mask*>—scan files matching the specified mask. By default, all files are scanned.

/FR:<*regexpr*>—scan files matching the specified regular expression. By default, all files are scanned.

/FULL—perform a full scan of all hard drives and removable media (including boot sectors). If additional parameters are set (for example, objects to be scanned or /TM and /TB parameters), an express scan will be performed, and the specified objects will be scanned. (For Scanner only.)

/FX:<*mask*>—exclude from scan files that match the specified mask. (For Console Scanner only.)

/GO—Scanner operation mode that skips the questions that require answers from a user; decisions that require a selection are made automatically. This mode is useful for the automatic file scanning; for example, for the daily or weekly hard disc scanning. An object for scanning must be indicated in the command line. Along with the /GO parameter, it is also possible to use the following parameters: /LITE, /FAST, /FULL. In this mode, the scanning stops when switching to the battery power.

/H or /?—show brief help. (For Console Scanner only.)

/HA—use heuristic analysis to detect unknown threats. Option is enabled by default.

/KEY:<*key_file*>—specify a path to the key file. It is necessary to use this parameter if your key file is stored outside of the installation folder where the scanner executables reside. By default, drweb32.key or another suitable file from the C:\Program Files\DrWeb\ folder is used.

/LITE—perform a basic scan of random access memory and boot sectors of all disks as well as run a scan for rootkits. (For Scanner only.)

/LN—resolve shell links. Option is disabled by default.

/LS—scan using LocalSystem account rights. Option is disabled by default.

/MA—scan mail files.

/MC:<*number_of_attempts*>—set the maximum number of cure attempts. By default: unlimited.

/NB—do not backup cured or deleted files. Option is disabled by default.

`/NI[:X]`—limits usage of system resources at scanning (%), defines the amount of memory required for scanning and the priority of scanning process. By default: unlimited.

`/NOREBOOT`—cancel system reboot or shutdown after scanning. (For Scanner only.)

`/NT`—scan NTFS streams.

`/OK`—show the full list of scanned objects and mark clean files with `Ok.` Option is disabled by default.

`/P:`<*priority*>—priority of the current scanning task. Can be as follows:

0—the lowest

L—low

N—normal (default priority)

H—high

M—maximal

`/PAL:`<*nesting_level*>—maximum nesting level for executable packers. If a nesting level is greater than the specified value, scanning proceeds until this limit is reached. The nesting level is 1,000 by default.

`/QL`—show the list of files quarantined on all disks. (For Console Scanner only.)

`/QL:`<*logical_drive_letter*>—show the list of files quarantined on the specified logical drive. (For Console Scanner only.)

`/QNA`—double quote paths.

`/QR[:[d][:p]]`—delete quarantined files on drive <*d*> *(logical_drive_letter)* that are older than <*p*> *(number)* days. If <*d*> and <*p*> are not specified, all quarantined files on all drives are deleted. (For Console Scanner only.)

`/QUIT`—terminate Scanner once scanning is complete regardless of whether or not any actions have been applied to the detected threats. (For Scanner only.)

`/RA:`<*file_name*>—append the report on program operation to the specified file. By default, logging is disabled.

`/REP`—follow symbolic links while scanning. Option is disabled by default.

`/RK`—scan for rootkits. Option is disabled by default.

`/RP:`<*file_name*>—write the report on program operation to the specified file. By default, logging is disabled.

`/RPC:`<*sec*>—Scanning Engine connection timeout. Timeout is 30 seconds by default. (For Console Scanner only.)

/RPCD—use dynamic RPC identification. (For Console Scanner only.)

/RPCE—use dynamic RPC endpoint. (For Console Scanner only.)

/RPCE:<*target_address*>—use specified RPC endpoint. (For Console Scanner only.)

/RPCH:<*host_name*>—use specified host name for remote call. (For Console Scanner only.)

/RPCP:<*protocol*>—use specified RPC protocol. Possible protocols are as follows: lpc, np, tcp. (For Console Scanner only.)

/SCC—show content of complex objects. Option is disabled by default.

/SCN—show installation package name. Option is disabled by default.

/SLS—show logs on the screen. Option is enabled by default. (For Console Scanner only.)

/SPN—show packer name. Option is disabled by default.

/SPS—display scan progress on the screen. Option is enabled by default. (For Console Scanner only.)

/SST—display object scan time. Option is disabled by default.

/ST—start of Scanner in the background mode. If the /GO parameter is not set, the graphical mode is displayed only in case of threat detection. In this mode, the scanning stops when switching to the battery power.

/TB—scan boot sectors including master boot record (MBR) of the hard drive.

/TM—scan processes in memory including Windows system control area.

/TR—scan system restore points.

/W:<*sec*>—maximum time to scan (sec.). By default: unlimited.

/WCL—drwebwcl compatible output. (For Console Scanner only.)

/X:S[:R]—set one of the following states for the computer to enter once scanning is complete: Shutdown/Reboot/Suspend/Hibernate.

The following actions can be specified for different objects ('C'—cure, 'Q'—move to quarantine, 'D'—delete, 'I'—ignore, 'R'—inform; 'R' is available for Console Scanner only; 'R' is set by default for all objects in Console Scanner):

- /AAD:<*action*>—action for adware (possible: DQIR)
- /AAR:<*action*>—action for infected archives (possible: DQIR)
- /ACN:<*action*>—action for infected installation packages (possible: DQIR)
- /ADL:<*action*>—action for dialers (possible: DQIR)

- /AHT:<*action*>—action for hacktools (possible: DQIR)
- /AIC:<*action*>—action for incurable files (possible: DQR)
- /AIN:<*action*>—action for infected files (possible: CDQR)
- /AJK:<*action*>—action for jokes (possible: DQIR)
- /AML:<*action*>—action for infected mail files (possible: QIR)
- /ARW:<*action*>—action for riskware (possible: DQIR)
- /ASU:<*action*>—action for suspicious files (possible: DQIR)

Several switches can have modifiers that explicitly enable or disable options specified by these switches. For example, as follows:

/AC– option is clearly disabled

/AC, /AC+ option is clearly enabled.

These modifiers can be useful if the option was enabled or disabled by default or was set in the configuration file earlier. The following switches can have modifiers:

/AC, /AFS, /AR, /BI, /DR, /HA, /LN, /LS, /MA, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SLS, /SPN, /SPS, /SST, /TB, /TM, /TR, /WCL.

For /FL parameter '–' modifier directs to scan the paths listed in the specified file and then delete this file.

For /ARC, /ARL, /ARS, /ART, /ARX, /NI[:X], /PAL, /RPC, /W parameters "0" value means that there is no limit.

The following example shows how to use command-line switches with Console Scanner:

```
[<path_to_program>]dwscancl /AR- /AIN:C /AIC:Q C:\
```

scan all files on disk 'C:', excluding those in archives; cure the infected files and move to quarantine those that cannot be cured. To run Scanner the same way, enter the dwscancl command name instead of dwscanner.

Dr.Web Updater Command-Line Parameters

Common options

Parameter	Description
-h [--help]	Show a short help message on how to use the program.
-v [--verbosity] arg	Log level. Can be one of following: error (standard), info (extended), debug.
-d [--data-dir] arg	Directory where repository and settings are located.
--log-dir arg	Directory for storing the log file.
--log-file arg (=dwupdater.log)	Log file name.
-r [--repo-dir] arg	Repository directory, (<data_dir>/repo by default).
-t [--trace]	Enable tracing.
-c [--command] arg (=update)	Command to execute: getversions, getcomponents, init, update, uninstall, exec, keyupdate, and download.
-z [--zone] arg	Zones that are to be used instead of those specified in the configuration file.

init command parameters

Parameter	Description
-s [--version] arg	Version name.
-p [--product] arg	Product name.
-a [--path] arg	Product directory path. This folder will be used as the default directory for all components included in the product. Dr.Web Updater will search for a key file in this directory.
-n [--component] arg	Component name and installation folder specified as follows:<*name*>, <*install path*>.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
-g [--proxy] arg	Proxy server for updating. <*address*>:<*port*>.

Parameter	Description
-e [--exclude] arg	Component name that will be excluded from the product during installation.

update command parameters

Parameter	Description
-p [--product] arg	Product name. If specified, only this product will be updated. If neither a product nor certain components are specified, all products will be updated. If certain components are specified, only they will be updated.
-n [--component] arg	Components that should be updated to the specified version. *<Name>*, *<target revision>*.
-x [--selfrestart] arg (=yes)	Reboot after an update of Dr.Web Updater. Default value is `yes`. If the value is set to `no`, notification that reboot is required will appear.
--geo-update	Get the list of IP addresses from update.drweb.com before updating.
--type arg (=normal)	Can be one of the following: • Reset-all—forced update of all components • Reset-failed—reset revision for damaged components • Normal-failed—try to update all components including damaged from the current revision to the newest or specified • Update-revision—try to update all components of the current revision to the newest if exists • Normal—update all components
-g [--proxy] arg	Proxy server for updating. *<Address>*:*<port>*.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
--param arg	Pass additional parameters to the script. *<Name>*: *<value>*.
-l [--progress-to-console]	Print information about downloading and script execution to the console.

Getcomponents command parameters

Parameter	Description
-s [--version] arg	Version name.

Parameter	Description
-p [--product] arg	Specify the product to get the list of components that are included in this product. If the product is not specified, all components of this version will be listed.

getrevisions command parameters

Parameter	Description
-s [--version] arg	Version name.
-n [--component] arg	Component name.

uninstall command parameters

Parameter	Description
-n [--component] arg	Name of the component that is to be uninstalled.
-l [--progress-to-console]	Print information about command execution to the console.
--param arg	Pass additional parameters to the script. *<Name>: <value>*.
-e [--add-to-exclude]	Components to be deleted. Update of this components will not be performed.

keyupdate command parameters

Parameter	Description
-m [--md5] arg	MD5 hash of the previous key file.
-o [--output] arg	Output file name to store new key.
-b [--backup]	Backup of an old key file if exists.
-g [--proxy] arg	Proxy server for updating. *<Address>:<port>*.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.

Parameter	Description
-l [--progress-to-console]	Print information about downloading of the key file to the console.

download command parameters

Parameter	Description
--zones arg	Zone description file.
--key-dir arg	Directory where the key file is located.
-l [--progress-to-console]	Print information about command execution to the console.
-g [--proxy] arg	Proxy server for updating. <*Address*>:<*port*>.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
-s [--version] arg	Version name
-p [--product] arg	Name of the product to download.

Return Codes

The values of the return code and corresponding events are as follows:

Return code value	Event
0	OK, no virus found.
1	Known virus detected.
2	Modification of known virus detected.
4	Suspicious object found.
8	Known virus detected in file archive, mail archive, or container.
16	Modification of known virus detected in file archive, mail archive, or container.
32	Suspicious file found in file archive, mail archive, or container.

Return code value	Event
64	At least one infected object successfully cured.
128	At least one infected or suspicious file deleted/renamed/moved.

The actual value returned by the program is equal to the sum of codes for the events that occurred during scanning. Obviously, the sum can be easily decomposed into separate event codes.

For example, return code 9 = 1 + 8 means that known viruses were detected, including viruses in archives, mail archives or containers; curing and others actions were not executed; no other “virus” events occurred during scanning.

Appendix B. Computer Threats and Neutralization Methods

With the development of computer technologies and network solutions malicious programs (malware) of different kinds, meant to strafe users, become more and more widespread. Their development began together with computer science and facilities of protection against them progressed alongside. Nevertheless, there is still no common classification for all possible threats due to their unpredictable development character and constant improvement of applicable technologies.

Malicious programs can be distributed through the Internet, local area networks, email and portable data mediums. Some of them rely on the user’s carelessness and lack of experience and can be run in completely automatic mode. Others are tools controlled by a computer cracker and they can harm even the most secure systems.

This chapter describes all of the most common and widespread types of malware, against which products of Doctor Web are aimed.

Classification of Computer Threats

Herein, the term “threat” defines any kind of software that can potentially or directly inflict damage on a computer or network or compromise the user's information or rights (in other words, malicious and other unwanted programs). However, generally speaking, the term “threat” may be used to indicate any potential danger to computer or network security (that is, vulnerabilities that can be exploited to launch attacks).

All program types described below have the ability to endanger the user's data or confidentiality. Programs that do not hide their presence from the user (for example, spam-sending software or traffic analyzers) usually are not considered to be computer threats, although they can become threats under certain circumstances.

In the documentation and products by Doctor Web, threats are divided into two categories in accordance with the severity of danger they pose.

- **Major threats** are classic computer threats that can perform destructive or illegal actions in the system on their own (erase or steal important data, crash networks, and so on). To this type of computer threats belong programs that are traditionally referred to as “malicious” (viruses, worms, and Trojans).
- **Minor threats** are less dangerous than major threats, but may be used by a third party to carry out malicious activities. Moreover, mere presence of minor threats in the system indicates its low protection level. Information security specialists sometimes refer to this type of threats as “grayware” or potentially unwanted programs. This category consists of adware, dialers, jokes, riskware, and hacktools.

Major threats

Computer viruses

This type of computer threats is characterized by their ability to inject malicious code into running processes of other programs. This action is called *infection*. In most cases, the infected file becomes a virus carrier itself, and the injected code does not necessarily match the original one. The majority of viruses are created with a purpose to damage or destroy data in the system.

Doctor Web divides viruses by the type of objects they infect into the following categories:

- **File viruses** infect operating system files (usually, executable files and dynamic-link libraries) and are activated when an infected file is run.
- **Micro viruses** infect documents used by Microsoft® Office or other programs supporting macro commands (usually, written in Visual Basic). Macro commands are a type of built-in programs (macros) that are written in a fully functional programming language and can be launched under specific circumstances (for example, in Microsoft® Word, macros can be activated upon opening, closing, or saving a document).
- **Script viruses** are created using script languages, and, mostly, they infect other scripts (such as OS service files). By exploiting vulnerable scripts in web applications, they can also infect other file types that support script execution.
- **Boot viruses** infect boot sectors of disks and partitions or master boot records of hard disks. They require little memory and can perform their tasks until the operating system is rolled out, restarted, or shut down.

Most viruses have special mechanisms that protect them against detection. These mechanisms are constantly improved, and ways to overcome them are constantly developed. According to the type of protection they use, all viruses can be divided into two following groups:

- **Encrypted viruses** self-encrypt their malicious code upon every infection to make its detection in a file, boot sector, or memory more difficult. Each sample of such viruses contains only a short common code fragment (decryption procedure) that can be used as a virus signature.
- **Polymorphic viruses** use a special decryption procedure in addition to code encryption. This procedure is different in every new virus copy. This means that such viruses do not have byte signatures.

Viruses can also be classified according to the language they are written in (most viruses are written in Assembly, high-level programming languages, script languages, and so on) and operating systems that can be infected by these viruses.

Computer worms

Recently, worms have become much more widespread than viruses and other malicious programs. Like viruses, these malicious programs can replicate themselves. A worm infiltrates a computer from a network (usually, as an email attachment) and spreads its functional copies among other computers. Distribution can be triggered by some user action or automatically.

Worms do not necessarily consist of only one file (the worm's body). Many of them have a so-called infectious part (shellcode) that is loaded into the main memory. After that, it downloads the worm's body as an executable file via the network. If only the shellcode is present in the system, the worm can be easily removed by restarting the system (at that, RAM is reset). However, if the worm's body infiltrates the computer, only an anti-virus program can fight it.

Even if worms do not bear any payload (do not cause direct damage to a system), they can still cripple entire networks because of how intensely they spread.

Doctor Web classifies worms in accordance with their distribution methods as follows:

- **Network worms** spread via various network and file-sharing protocols.
- **Mail worms** spread via mail protocols (POP3, SMTP, and others).

Trojan programs (Trojans)

These programs cannot replicate themselves. However, they can perform malicious actions on their own (damage or delete data, forward confidential information, and others) or provide cybercriminals with authorized access to a computer to harm a third party.

Like viruses, these programs can perform various malicious activities, hide their presence from the user, and even be a virus component. However, usually, Trojans are distributed as separate executable files (through file-exchange servers, data carriers, or email attachments) that are run by users themselves or by some specific system process.

Here are some Trojan types divided by Doctor Web into separate categories as follows:

- **Backdoors** are Trojans that allow an intruder to get privileged access to the system bypassing any existing protection mechanisms. Backdoors do not infect files—they register themselves in the registry modifying registry keys.
- **Droppers** are file carriers that contain malicious programs in their bodies. Once launched, a dropper copies malicious files to a hard disk without user consent and runs them.
- **Keyloggers** can log data that users enter by means of a keyboard. These malicious programs can steal varies confidential information (including network passwords, logins, bank card data, and so on).
- **Clickers** redirect users to specified Internet resources (may be malicious) in order to increase traffic to those websites or to perform DoS attacks.
- **Proxy Trojans** provide cybercriminals with anonymous Internet access via the victim's computer.
- **Rootkits** are used to intercept operating system functions in order to hide their presence. Moreover, a rootkit can conceal processes of other programs, registry keys, folders, and files. It can be distributed either as an independent program or as a component of another malicious application. Based on the operation mode, rootkits can be divided into two following

categories: User Mode Rootkits (UMR) that operate in user mode (intercept functions of user-mode libraries) and Kernel Mode Rootkits (KMR) that operate in kernel mode (intercept functions at the system kernel level, which makes these malicious programs hard to detect).

Trojans can also perform other malicious actions besides those listed above. For example, they can change the browser home page or delete certain files. However, such actions can also be performed by threats of other types (viruses or worms).

Minor threats

Hacktools

Hacktools are designed to assist intruders with hacking. The most common among these programs are port scanners that detect vulnerabilities in firewalls and other components of computer protection system. Such tools can be used not only by hackers but also by administrators to check security of their networks. Sometimes various programs that use social engineering techniques are designated as hacktools too.

Adware

Usually, this term refers to a program code incorporated into freeware programs that forcefully display advertisements to users. However, sometimes such codes can be distributed via other malicious programs and show advertisements, for example, in web browsers. Many adware programs operate based on data collected by spyware.

Jokes

Like adware, this type of minor threats cannot be used to inflict any direct damage on the system. Joke programs usually just generate messages about allegedly detected errors and threaten to perform actions that may lead to data loss. Their purpose is to frighten or annoy users.

Dialers

These are special programs that, after asking for user's permission, employ Internet connection to access specific websites. Usually, these programs have a signed certificate and inform the user about all their actions.

Riskware

These programs are not intended to be computer threats. However, they can still cripple system security due to certain features and, therefore, are classified as minor threats. This type of threats includes not only programs that can accidentally damage or delete data but also programs that can be used by hackers or some malicious applications to harm the system. Among such programs are various remote chat and administrative tools, FTP-servers, and so on.

Suspicious objects

These are potential computer threats detected by the heuristic analyzer. Such objects can be any type of threat (even unknown to information security specialists) or turn out safe in case of a false detection. It is strongly recommended to move files containing suspicious objects to quarantine and send them for analysis to Doctor Web anti-virus laboratory.

Actions Applied to Threats

There are many methods of neutralizing computer threats. Products of Doctor Web combine these methods for the most reliable protection of computers and networks using flexible user-friendly settings and a comprehensive approach to security assurance. The main actions for neutralizing malicious programs are:

1. **Cure**—an action applied to viruses, worms and Trojans. It implies deletion of malicious code from infected files or deletion of a malicious program's functional copies as well as the recovery of affected objects (that is, return of the object's structure and operability to the state which was before the infection) if it is possible. Not all malicious programs can be cured. However, products of Doctor Web are based on most effective curing and file recovery algorithms.
2. **Move to quarantine**—an action when the malicious object is moved to a special folder and isolated from the rest of the system. This action is preferable in cases when curing is impossible and for all suspicious objects. It is recommended to send copies of such files to Doctor Web anti-virus laboratory.
3. **Delete**—the most effective action for neutralizing computer threats. It can be applied to any type of malicious objects. Note that deletion will sometimes be applied to certain files for which curing was selected. This will happen if the file contains only malicious code and no useful information. For example, curing of a computer worm implies deletion of all its functional copies.
4. **Block, rename**—these actions can also be used for neutralizing malicious programs. In the former case, all access attempts to or from the file are blocked. In the latter case, the extension of the file is renamed, which makes it inoperative.

Appendix C. Naming of Viruses

When Dr.Web components detect a threat, the notification in the user interface and the report file contain a name of the threat sample given by the specialists of Doctor Web anti-virus laboratory. These names are formed according to certain principles and reflect a threat's design, classes of vulnerable objects, distribution environment (OS and applications), and some other features. Knowing these principles may be useful for understanding software and organizational vulnerabilities of the protected system. The full and constantly updated version of this classification is available at http://vms.drweb.com/classification/.

In certain cases this classification is conventional as some viruses can possess several features at the same time. Besides, it should not be considered exhaustive as new types of viruses constantly appear, and the classification is made more precise.

The full name of a virus consists of several elements, separated by full stops. Some elements at the beginning of the full name (prefixes) and at the end of it (suffixes) are standard for the accepted classification.

Prefixes

Affected operating systems

The prefixes listed below are used for naming viruses infecting executable files of certain operating systems:

- `Win`—16-bit Windows 3.1 programs
- `Win95`—32-bit Windows 95/98/Me programs
- `WinNT`—32-bit Windows NT/2000/XP/Vista programs
- `Win32`—32-bit Windows 95/98/Me and NT/2000/XP/Vista programs
- `Win32.NET`—programs in Microsoft .NET Framework operating system
- `OS2`—OS/2 programs
- `Unix`—programs in various Unix-based systems
- `Linux`—Linux programs
- `FreeBSD`—FreeBSD programs
- `SunOS`—SunOS (Solaris) programs
- `Symbian`—Symbian OS (mobile OS) programs

Note that some viruses can infect programs of one system even if they are designed to operate in another system.

Macrovirus prefixes

The list of prefixes for viruses which infect MS Office objects (the language of the macros infected by such type of virus is specified):

- WM—Word Basic (MS Word 6.0-7.0)
- XM—VBA3 (MS Excel 5.0-7.0)
- W97M—VBA5 (MS Word 8.0), VBA6 (MS Word 9.0)
- X97M—VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0)
- A97M—databases of MS Access'97/2000
- PP97M—MS PowerPoint presentations
- O97M—VBA5 (MS Office'97), VBA6 (MS Office 2000); this virus infects files of more than one component of MS Office

Development languages

The HLL group is used to name viruses written in high-level programming languages, such as C, C++, Pascal, Basic, and others. To specify functioning algorithms, the following modifiers can be used:

- HLLW—worms
- HLLM—mail worms
- HLLO—viruses overwriting the code of the victim program
- HLLP—parasitic viruses
- HLLC—companion viruses

The following prefix also refers to development language:

- Java—viruses designed for the Java virtual machine

Trojan programs (Trojans)

Trojan—a general name for different Trojan programs (Trojans). In many cases the prefixes of this group are used with the Trojan prefix.

- PWS—password stealing Trojan
- Backdoor—Trojan with RAT-function (Remote Administration Tool—a utility for remote administration)
- IRC—Trojan which uses Internet Relay Chat channels
- DownLoader—Trojan which secretly downloads different malicious programs from the Internet
- MulDrop—Trojan which secretly downloads different viruses contained in its body
- Proxy—Trojan which allows a third-party user to work anonymously in the Internet via the infected computer

- StartPage (synonym: Seeker)—Trojan which makes unauthorized replacement of the browser home page address (start page)
- Click—Trojan which redirects a user's browser to a certain website (or websites)
- KeyLogger—a spyware Trojan which logs key strokes; it may send collected data to a malefactor
- AVKill—terminates or deletes anti-virus programs, firewalls, etc.
- KillFiles, KillDisk, DiskEraser—deletes certain files (all files on drives, files in certain directories, files by certain mask, etc.)
- DelWin—deletes files vital for the operation of Windows OS
- FormatC—formats drive C (synonym: FormatAll—formats all drives)
- KillMBR—corrupts or deletes master boot records (MBR)
- KillCMOS—corrupts or deletes CMOS memory

Tool for attacking vulnerabilities

- Exploit—a tool exploiting known vulnerabilities of an OS or application to implant malicious code or perform unauthorized actions

Tools for network attacks

- Nuke—tools for network attacks on known vulnerabilities of operating systems leading to abnormal shutdowns of the attacked system
- DDoS—agent program for performing a DDoS attack (Distributed Denial Of Service)
- FDoS (synonym: Flooder)—Flooder Denial Of Service—programs for performing malicious actions in the Internet which use the idea of DDoS attacks; in contrast to DDoS, when several agents on different computers are used simultaneously to attack one victim system, an FDoS program operates as an independent "self-sufficient" program (Flooder Denial of Service).

Script viruses

Prefixes of viruses written in different scrip languages:

- VBS—Visual Basic Script
- JS—Java Script
- Wscript—Visual Basic Script and/or Java Script
- Perl—Perl
- PHP—PHP
- BAT—MS-DOS command interpreter

Malicious programs

Prefixes of malicious programs that are not viruses:

- Adware—an advertising program
- Dialer—a dialer program (redirecting modem calls to predefined paid numbers or paid resources)
- Joke—a joke program
- Program—a potentially dangerous program (riskware)
- Tool—a program used for hacking (hacktool)

Miscellaneous

Generic—this prefix is used after another prefix describing the environment or the development method to name a typical representative of this type of viruses. Such virus does not possess any characteristic features (such as text strings, special effects, etc.) which could be used to assign it some specific name.

Silly—this prefix was used with different modifiers to name simple featureless viruses in the past.

Suffixes

Suffixes are used to name some specific virus objects:

- generator—an object which is not a virus but a virus generator.
- based—a virus which is developed with the help of the specified generator or a modified virus. In both cases the names of this type are generic and can define hundreds and sometimes even thousands of viruses.
- dropper—an object which is not a virus but an installer of the given virus.